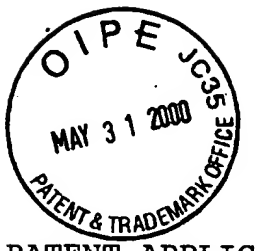


#6
KMS
5-7-00

35.G2550

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: Unknown
SATORU WAKAO, ET AL.	)	
	:	Group Art Unit: Unknown
Appln. No.: 09/521,424	)	
	:	
Filed: March 8, 2000	)	
	:	
For: IMAGE PROCESSING APPARATUS AND IMAGE PROCESSING METHOD	)	May 31, 2000

Assistant Commissioner For Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicants hereby claim priority under the International Convention and all rights to which they are entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Applications:

11-063174, filed March 10, 1999; and

2000-057077, filed March 2, 2000.

A certified copy of the priority document is enclosed.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicants

Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK/fdb

SATORU WAKAO, ET AL
Appln. No. 09/521,4

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年 ３月１０日

出願番号
Application Number: 平成１１年特許願第０６３１７４号

出願人
Applicant (s): キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ３月３１日

特許庁長官
Commissioner,
Patent Office 近藤隆

出証番号 出証特２０００－３０２２３８２

【書類名】　特許願

【整理番号】　3858035

【提出日】　平成11年 3月10日

【あて先】　特許庁長官　伊佐山　建志　殿

【国際特許分類】　G06F 15/00

H04N 7/00

【発明の名称】　画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体

【請求項の数】　42

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【氏名】　若尾　聡

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【氏名】　岩村　恵市

【特許出願人】

【識別番号】　000001007

【住所又は居所】　東京都大田区下丸子３丁目３０番２号

【氏名又は名称】　キヤノン株式会社

【代表者】　御手洗　冨士夫

【電話番号】　03-3758-2111

【代理人】

【識別番号】　100069877

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【弁理士】

【氏名又は名称】　丸島　儀一

【電話番号】　03-3758-2111

【手数料の表示】

【予納台帳番号】　011224

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9703271

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項１】　ディジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、

前記演算手段の出力を用いて、前記ディジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする画像処理装置。

【請求項２】　請求項１において、前記演算手段は、前記ディジタル画像と前記秘密情報とを用いて逆演算可能な演算を行うことを特徴とする画像処理装置。

【請求項３】　請求項１若しくは２において、前記生成手段は、前記演算手段の演算結果に対して一方向関数を用いた演算を行うことを特徴とする画像処理装置。

【請求項４】　請求項３において、前記一方向性関数は、ハッシュ関数であることを特徴とする画像処理装置。

【請求項５】　請求項３において、前記一方向性関数は、共通鍵暗号を実現する関数であることを特徴とする画像処理装置。

【請求項６】　請求項１～５の何れかにおいて、前記生成手段は、前記ディジタル画像毎に、該ディジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項７】　請求項１～６の何れかにおいて、前記生成手段は、前記演算手段の出力を用いて、前記ディジタル画像に対する不正な処理を検出するため署名データを生成するプログラムに従って前記ディジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項８】　請求項１～７の何れかにおいて、前記秘密情報は、前記画像処理装置を識別するための情報であることを特徴とする画像処理装置。

【請求項９】　請求項１～７の何れかにおいて、前記秘密情報は、前記画像処理装置と接続可能な外部装置を識別するための情報であることを特徴とする画像処理装置。

【請求項１０】　請求項１～７の何れかにおいて、前記秘密情報は、前記画像処理装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする画像処理装置。

【請求項１１】　請求項１～１０の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記画像処理装置に接続された外部装置に演算させることを特徴とする画像処理装置。

【請求項１２】　請求項１～１１の何れかにおいて、前記ディジタル画像は、圧縮符号化されていることを特徴とする画像処理装置。

【請求項１３】　請求項１～１２の何れかにおいて、前記画像処理装置は更に、前記ディジタル画像を生成する撮像部を具備することを特徴とする画像処理装置。

【請求項１４】　請求項１～１３の何れかにおいて、前記画像処理装置は更に、前記ディジタル画像と前記署名データとを出力可能なディジタルインタフェースを具備することを特徴とする画像処理装置。

【請求項１５】　請求項１～１４の何れかにおいて、前記画像処理装置は更に、前記前記ディジタル画像データと前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする画像処理装置。

【請求項１６】　ディジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、

前記演算手段の出力と、前記ディジタル画像に対する不正な処理を検出するための署名データとを比較して前記ディジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする画像処理装置。

【請求項１７】　請求項１６において、前記演算手段は、前記ディジタル画像と前記秘密情報とを用いて逆演算可能な第１の演算を行うことを特徴とする画像処理装置。

【請求項１８】　請求項１７において、前記演算手段は、前記第１の演算の結果に対して一方向関数を用いた第２の演算を行うことを特徴とする画像処理装置。

【請求項１９】　請求項１６～１８の何れかにおいて、前記画像処理装置は、前記ディジタル画像毎に、該ディジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項２０】　請求項１６～１９の何れかにおいて、前記検出手段は、前記演算手段の出力と前記署名データとを比較して前記ディジタル画像に対する不正な処理の有無を検出するプログラムに従って前記ディジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項２１】　請求項１６～２０の何れかにおいて、前記画像処理装置は更に、前記検出手段の検出結果を表示する表示手段を具備することを特徴とする画像処理装置。

【請求項２２】　ディジタル画像と秘密情報とを用いて所定の演算を行う第１の演算手段と、

前記第１の演算手段の出力を用いて、該ディジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第１の画像処理装置と、

前記ディジタル画像と前記秘密情報とを用いて所定の演算を行う第２の演算手段と、

前記第２の演算手段の出力と前記署名データとを比較して該ディジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第２の画像処理装置とにより構成することを特徴とする画像処理システム。

【請求項２３】　ディジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記ディジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする画像処理方法。

【請求項２４】　ディジタル画像と秘密情報とを用いて所定の演算を行い、

該演算結果と、前記ディジタル画像に対する不正な処理を検出するための署名データとを比較して前記ディジタル画像に対する不正な処理の有無を検出するこ

とを特徴とする画像処理方法。

【請求項２５】　ディジタル画像と秘密情報とを用いて所定の演算を行う手順と、

該演算結果を用いて、前記ディジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項２６】　ディジタル画像と秘密情報とを用いて所定の演算を行う手順と、

該演算結果と、前記ディジタル画像に対する不正な処理を検出するための署名データとを比較して前記ディジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項２７】　ディジタル画像を生成する撮像手段と、

前記ディジタル画像と秘密情報とを用いて所定の演算を行い、該ディジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする撮像装置。

【請求項２８】　請求項２７において、前記生成手段は、前記ディジタル画像と前記秘密情報とを用いて逆演算可能な第１の演算を行うことを特徴とする画像処理装置。

【請求項２９】　請求項２８において、前記生成手段は、前記第１の演算の結果に対して一方向関数を用いた第２の演算を行うことを特徴とする画像処理装置。

【請求項３０】　請求項２９において、前記一方向性関数は、ハッシュ関数であることを特徴とする撮像装置。

【請求項３１】　請求項２９において、前記一方向性関数は、共通鍵暗号を実現する関数であることを特徴とする撮像装置。

【請求項３２】　請求項２９において、前記生成手段は、前記撮像手段が前記ディジタル画像を生成する毎に、該ディジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項３３】　請求項２７～３２の何れかにおいて、前記生成手段は、前記撮像手段により生成されたディジタル画像と秘密情報とを用いて所定の演算を行い、該ディジタル画像に対する不正な処理を検出するための署名データを生成するプログラムに従って前記ディジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項３４】　請求項２７～３３の何れかにおいて、前記秘密情報は、前記撮像装置を識別するための情報であることを特徴とする撮像装置。

【請求項３５】　請求項２７～３３の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を識別するための情報であることを特徴とする撮像装置。

【請求項３６】　請求項２７～３３の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする撮像装置。

【請求項３７】　請求項２７～３６の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記撮像装置に接続された外部装置に演算させることを特徴とする撮像装置。

【請求項３８】　請求項２７～３７の何れかにおいて、前記ディジタル画像は、圧縮符号化されていることを特徴とする撮像装置。

【請求項３９】　請求項２７～３８の何れかにおいて、前記撮像装置は更に、前記ディジタル画像と前記署名データとを出力可能なディジタルインタフェースを具備することを特徴とする撮像装置。

【請求項４０】　請求項２７～３９の何れかにおいて、前記撮像装置は更に、前記前記ディジタル画像と前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする撮像装置。

【請求項４１】　ディジタル画像を撮像し、

該ディジタル画像と秘密情報とを用いて所定の演算を行い、

該ディジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする撮像方法。

【請求項４２】　撮像部により撮像されたディジタル画像と、秘密情報とを用いて所定の演算を行う手順と、

該ディジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体に係り、特にディジタル画像情報の著作権を保護するための技術、ディジタル画像情報に対する不正な処理を検出するための技術に関するものである。

【０００２】

【従来の技術】

近年、撮影した画像を従来の銀塩写真や８ｍｍフィルムに記録するのではなく、ディジタルデータとして記録媒体に記録する画像入力装置（例えば、デジタルカメラ）が実用化されている。

【０００３】

【発明が解決しようとする課題】

ところが、通常ディジタルデータは、アナログデータと異なり加工が容易で、改竄、偽造、合成等を簡単に行うことができる。このため、ディジタルデータは、銀塩写真等と比較して信憑性が低く、証拠能力に乏しいという問題があった。

【０００４】

このような問題を解決するために、ディジタルデータに対する改竄、偽造、合成等を検出するための技術が提案されている。例えば、この技術の一例として、ハッシュ関数と公開鍵暗号方式とを組み合わせたシステムが提案されている。

【０００５】

以下、図２８を用いてそのシステムを説明する。ここで、公開鍵暗号方式は、暗号鍵と復号鍵とが異なり、暗号鍵を公開し、復号鍵を秘密に保持する方式であ

る。

【０００６】

まず、送信側（出力側）の構成と動作について説明する。

【０００７】

①ディジタルデータＭをハッシュ関数Ｈを用いて圧縮し、一定長の出力ｈを演算する。

【０００８】

②暗号鍵Ｋｅを用いて上述のｈを暗号化し、出力ｓを求める。この出力ｓをディジタル署名データと呼ぶ。

【０００９】

③出力回路は、ディジタル署名データｓとディジタルデータＭとを一組として出力する。

【００１０】

次に、受信側（検出側）構成と動作について説明する。

【００１１】

④ディジタルデータＭとそれに対応するディジタル署名データｓとを入力する。

【００１２】

⑤ディジタル署名データｓを暗号鍵Ｋｅに対応する復号鍵Ｋｄで復号し、出力ｈ’’を生成する。

【００１３】

⑥ディジタルデータＭを送信側と同じハッシュ関数Ｈを用いて演算し、出力ｈ’を求める。

【００１４】

⑦比較回路は、⑤で求めた出力ｈ’’と⑥で求めた出力ｈ’とを比較し、一致すれば入力されたディジタルデータＭを不正な処理のされていない正当なデータであると判断し、不一致であれば不正な処理のされたデータと見なす。

【００１５】

つまり、ハッシュ関数Ｈと暗号鍵Ｋｅとを用いてディジタル署名データｓを生

成することによって、ディジタルデータMに対する改竄、偽造、合成等を検出することができる。

【００１６】

しかしながら、上述のシステムには次のような問題があった。

【００１７】

例えば、公開鍵暗号方式の暗号化回路及び復号化回路の構成は複雑で小型化が難しく、それらの回路の演算量は膨大で、処理時間が長くなる欠点があった。特に、公開鍵暗号方式では、べき乗演算と剰余演算とが必要であり、共通鍵暗号方式（暗号鍵と復号鍵とが同一となる暗号方式）に比べて演算が複雑且つ膨大となるため、処理の高速化が大変難しかった。そのため、高速な処理の実現は難しく、小型で安価なシステムをユーザに提供しにくい問題があった。

【００１８】

又、処理時間を早くするためには、より高性能のＣＰＵ（中央演算処理装置）とより大容量のメモリとを用いて、ハードウェアの性能を向上させる必要がある。しかしながら、それではシステム全体の大規模化やコストアップを招くだけで安価で小型で高速なシステムをユーザに提供しにくい問題があった。

【００１９】

以上の背景から本出願の発明の目的は、ディジタルデータの著作権を保護すると共に、そのディジタルデータに対する不正な処理を簡単な構成で、高速に検出することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【００２０】

又、本出願の発明の目的は、ディジタルデータの著作権を保護すると共に、そのディジタルデータが不正に処理されていないことを検証するためのデータを簡単な構成で、高速に生成することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【００２１】

又、本出願の発明の目的は、ディジタルデータが不正に処理されていないこと

を検証するためのデータを用いて、そのディジタルデータに対する不正な処理を簡単な構成で、高速に検出することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【００２２】

【課題を解決するための手段】

上述のような目的を達成するために、本発明の画像処理装置は、ディジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力を用いて、前記ディジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【００２３】

又、本発明の画像処理装置は、ディジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力と、前記ディジタル画像に対する不正な処理を検出するための署名データとを比較して前記ディジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする。

【００２４】

又、本発明の画像処理システムは、ディジタル画像と秘密情報とを用いて所定の演算を行う第１の演算手段と、前記第１の演算手段の出力を用いて、該ディジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第１の画像処理装置と、前記ディジタル画像と前記秘密情報とを用いて所定の演算を行う第２の演算手段と、前記第２の演算手段の出力と前記署名データとを比較して該ディジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第２の画像処理装置とにより構成することを特徴とする。

【００２５】

又、本発明の画像処理方法は、ディジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記ディジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【００２６】

又、本発明の画像処理方法は、ディジタル画像と秘密情報とを用いて所定の演

算を行い、該演算結果と、前記ディジタル画像に対する不正な処理を検出するための署名データとを比較して前記ディジタル画像に対する不正な処理の有無を検出することを特徴とする。

【００２７】

又、本発明のコンピュータ読み取り可能な記憶媒体は、ディジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果を用いて、前記ディジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【００２８】

又、本発明のコンピュータ読み取り可能な記憶媒体は、ディジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果と、前記ディジタル画像に対する不正な処理を検出するための署名データとを比較して前記ディジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【００２９】

又、本発明の撮像装置は、ディジタル画像を生成する撮像手段と、前記ディジタル画像と秘密情報とを用いて所定の演算を行い、該ディジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【００３０】

又、本発明の撮像方法は、ディジタル画像を撮像し、該ディジタル画像と秘密情報とを用いて所定の演算を行い、該ディジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【００３１】

又、本発明のコンピュータ読み取り可能な記憶媒体は、撮像部により撮像されたディジタル画像と、秘密情報とを用いて所定の演算を行う手順と、該ディジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【００３２】

【発明の実施の形態】

以下、本発明の画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体について図面を用いて詳細に説明する。

【００３３】

（基本構成）

まず、図１を用いて、各実施例に共通するディジタル画像検証システムの基本構成と処理手順とについて説明する。

【００３４】

図１において、画像入力装置１０は、ディジタル画像データＰ１１と秘密情報Ｓ１２とに基づいてディジタル署名データｈ１３を生成する。具体的に、画像入力装置１０は、秘密情報Ｓ１２を用いてディジタル画像データＰ１１にある操作（例えば、付加、多重、或いは合成）を加え、その結果を一方向性関数（例えば、ハッシュ関数等の逆関数の生成が困難或いは不可能な関数）で演算し、その演算結果からディジタル署名データｈ１３を生成する。このディジタル署名データｈ１３は、対応するディジタル画像データＰ１１と共に一時的に記録され、必要に応じて外部出力される。

【００３５】

又、図１において、画像検証装置２０は、ディジタル画像データＰ’２１と共にディジタル署名データｈ’２３を外部入力する。画像検証装置２０は、ディジタル画像データＰ’２１と秘密情報Ｓ２２（上述の秘密情報Ｓ１２と同一の情報である）とを用いて画像入力装置１０と同様の処理を行い、ディジタル署名データｈ’’２４を生成する。

【００３６】

このディジタル署名データｈ’’２４は、ディジタル画像データＰ’２１と共に外部入力されたディジタル署名データｈ’２３と比較される。両者が一致した場合、画像検証装置２０は、ディジタル画像データＰ’２１を不正な処理のされていない正当なデータであると判断する。又、ディジタル画像データＰ’２１が外部入力される前に改竄されていた場合、両者は不一致となるため、ディジタル画

像データＰ’２１を不正に処理されたデータであると判断する。このような手順により、画像検証処装置２０は、外部入力されたディジタル画像データＰ’２１に対して不正な処理（例えば、改竄、偽造、合成等）が施されているか否かを検出することができる。

【００３７】

尚、図１において、画像入力装置１０と画像検証装置２０とは、同一の秘密情報を共有する。この秘密情報は、読み出し専用の記録媒体等に記録され、外部に漏れることがないように管理されている。

【００３８】

以上のように、本実施例のディジタル画像検証システムでは、秘密情報Ｓ１２を用いてディジタル画像データＰ１１にある操作を加え、その結果を一方向性関数演算し、その演算結果からディジタル署名データｈ１３を生成している。

【００３９】

このような処理によって得られたディジタル署名データｈ１３は、ディジタル画像データＰ１１と秘密情報Ｓ１２とに対して固有の情報となるため、不正なユーザは、秘密情報Ｓ１２を知らなければ、ディジタル画像データＰ１１を改竄したとしても、そのディジタル画像データＰ１１に対応するディジタル署名データｈ１３を不正に作り出すことはできない。又、不正なユーザは、一方向性関数の性質により、得られたディジタル署名データｈ１３から元のデータ（即ち、秘密情報Ｓ１２を用いてある操作を加えたディジタル画像データＰ１１）を知ることもできない。

【００４０】

これにより、本実施例では、複雑な暗号化技術を用いることなく、簡単で安価な回路構成と少ない演算量で高速にディジタル署名データを生成することができ、ディジタル画像データの著作権を保護し、該ディジタル画像データに対する不正な処理（改竄、偽造、合成等）を確実に検出することができる。

【００４１】

次に、図１に示す画像入力装置１０及び画像検証装置２０の基本構成について詳細に説明する。

【００４２】

（１）画像入力装置の構成

図２は、画像入力装置１０の構成の一例を示す図である。ここで、画像入力装置１０は、デジタルカメラ、カメラ一体型デジタルレコーダ、スキャナ等の撮像機能を有する電子機器である。

【００４３】

図２において、撮像部２０１は、ＣＣＤやレンズ等からなり、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのディジタル画像データに変換する。作業用メモリ２０２は、ディジタル画像データ等を一時的に保管し、ディジタル画像データに対する高能率符号化処理、後述のディジタル署名データの生成等に使用される。

【００４４】

記録再生部２０３は、取り外し可能な記録媒体（例えば、メモリカード等）を有し、撮像部２０１により生成され、高能率符号化されたディジタル画像データとそれに対応するディジタル署名データとを一組として記録する。駆動部２０４は、撮像部２０１や記録再生部２０３の機械的動作を制御する。

【００４５】

外部インタフェース部２０５は、１つ以上の外部装置と接続可能なディジタルインタフェースであり、例えば、ディジタル署名データの付加されたディジタル画像データを所定の外部装置に送信することができる。

【００４６】

制御／演算部２０６は、ＲＯＭ２０７に格納されている各種のプログラムに従って画像入力装置全体の動作を制御する制御回路２１０、ディジタル画像データを高能率符号化（例えば、ＤＣＴ変換やウェーブレット変換されたディジタル画像データを量子化し、可変長符号化する）する画像処理回路２１１、後述のディジタル署名データの生成に必要なハッシュ関数演算や各種の演算処理を行う演算回路２１２、ディジタル署名データの生成に必要な秘密情報（例えば、画像入力装置１０を識別するためのＩＤ情報等）を格納するメモリ２１３、演算回路２１２に必要な乱数を生成する乱数発生回路２１４を含む。

【００４７】

ＲＯＭ２０７は読み出し専用メモリであり、画像入力装置１０全体の動作を制御するプログラム、画像処理を制御するプログラム、ディジタル著名データを生成処理を制御するプログラム等を格納している。操作部２０８は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部２０６に供給する。

【００４８】

（２）画像検証装置の構成

図３は、画像検証装置２０の構成の一例を示す図である。ここで、画像検証装置２０は、パーソナルコンピュータ、ワークステーション等の情報処理装置やそれに接続可能な拡張ボードである。

【００４９】

図３において、外部インタフェース部３０１は、外部のネットワークからディジタル署名データの付加されたディジタル画像データ（ここで、ディジタル画像データは、高能率符号化されている）を入力するディジタルインタフェースである。又、外部インタフェース部３０１は、取り外し可能な記録媒体（例えば、メモリカード等）とも接続可能である。そして、その記録媒体に記録されたディジタル画像データをディジタル署名データと共に入力する。

【００５０】

作業用メモリ３０２は、ディジタル画像データ等を一時的に保管し、ディジタル画像データに対する伸長復号処理、後述のディジタル署名データの生成等に使用される。

【００５１】

制御／演算部３０３は、ＲＯＭ３０５に格納されている各種のプログラムに従って画像検証装置全体の動作を制御する制御回路３１０、ディジタル画像データを伸長復号（例えば、可変長復号し、逆量子化した後、逆ＤＣＴ変換や逆ウェーブレット変換する）する画像処理回路３１１、後述のディジタル署名データの生成に必要なハッシュ関数演算やディジタル画像データを検証するための演算処理を行う演算回路３１２、ディジタル署名データの生成に必要な秘密情報を格納す

るメモリ３１３、演算回路３１２に必要な乱数を生成する乱数発生回路３１４を含む。

【００５２】

表示部３０４は、ディジタル画像データを視覚的に表示する。又、表示部３０４は、そのディジタル画像データの検証結果をユーザに視覚的に表示できる。尚、表示部３０４は、画像検証装置２０と取り外し可能である。

【００５３】

ＲＯＭ３０５は、読み出し専用メモリであり、画像検証装置２０全体の動作を制御するプログラム、画像処理を制御するプログラム、ディジタル画像データの検証処理を制御するプログラムを格納している。操作部３０６は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部３０３に供給する。

【００５４】

以下、第１～第６の実施例では、図２の画像入力装置１０が、ディジタル画像データと秘密情報とに基づいてディジタル署名データを生成する手順について詳細に説明する。

【００５５】

又、第７～第１２の実施例では、図３の画像検証装置２０が、画像入力装置１０にて生成されたディジタル署名データに基づいてディジタル画像データの正当性を検証する手順について詳細に説明する。

【００５６】

（第１の実施例）

第１の実施例では、画像入力装置１０が、機器固有の秘密情報とハッシュ関数とを用いてディジタル署名データを生成する処理について説明する。具体的に第１の実施例では、ディジタル画像データと機器固有の秘密情報とを用いて予め定められた規則の演算を行い、その演算結果をハッシュ関数を用いて演算し、その演算結果をディジタル画像データに対するディジタル署名データとする。

【００５７】

図４は、第１の実施例の処理手順を説明するフローチャートである。以下、図

４に基づいて、ユーザの撮影指示からディジタル署名データの生成までの手順について説明する。

【００５８】

ステップＳ４０１において、操作部２０８は、ある被写体の光学像を撮像するか否かを指示する。撮像が指示された場合、制御／演算部２０６はステップＳ４０２を実行する。

【００５９】

ステップＳ４０２において、撮像部２０１は、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのディジタル画像データを生成する。その後、ディジタル画像データは、作業用メモリ２０２に格納される。

【００６０】

ステップＳ４０３において、制御／演算部２０６（に含まれる画像処理回路２１１）は、作業用メモリ２０２に格納されたディジタル画像データを１画面分の静止画像毎に高能率符号化する。ここで、１つの静止画像を高能率符号化する手法として例えば、複数画素からなるブロック毎にＤＣＴ変換、量子化及び可変量符号化するＤＣＴ変換方式、そのブロック毎にウェーブレット変換、量子化及び可変長符号化するウェーブレット変換方式、ＪＰＥＧ方式、ＪＢＩＧ方式、ＭＨ方式、ＭＭＲ方式、ＭＰＥＧ方式等を用いてもよい。尚、以下の実施例では、ＪＰＥＧ方式を用いて高能率符号化する場合について説明する。

【００６１】

ステップＳ４０４において、制御／演算部２０６は、画像入力装置１０の持つ固有の秘密情報をメモリ２１３から読み出す。

【００６２】

ステップＳ４０５において、制御／演算部２０６（に含まれる演算回路２１２）は、上述の秘密情報と例えばＪＰＥＧ方式で高能率符号化されたディジタル画像データ（以下、ＪＰＥＧデータと称する）とを用いて、予め定められた規則に基づく所定の演算処理を行う。

【００６３】

ここで、秘密情報と所定の演算処理とについて説明する。

【００６４】

まず、秘密情報とは、画像入力機器１０の製造時に設定される機器固有の情報であり、一般に公開されることのない情報である。この秘密情報は、外部から容易に入手することができないように制御／演算部２０６の内部に組み込まれている。以下、第１の実施例では、上述の秘密情報を例えば“１１１１１１１１”として説明する。尚、この秘密情報は、画像検証装置２０のもつ固有の秘密情報と共有できるものであればいかなるデータであってもよい。

【００６５】

次に、上述の所定の演算処理について説明する。所定の演算処理とは、図５に示すように、あるＪＰＥＧデータ列から所定の位置のバイトデータを選択し、そのバイトデータと秘密情報とをビット毎に排他的論理和演算することによってそのバイトデータを別のデータに変換する処理のことである。ここで、所定の位置とは、ＪＰＥＧデータ列上の任意の位置に設定することができるが、第１の実施例では最上位のバイトデータを演算対象とする。

【００６６】

ステップＳ４０６において、制御／演算部２０６（に含まれる演算回路２１２）は、所定の演算処理の施されたＪＰＥＧデータをハッシュ関数を用いて演算し、ディジタル署名データを生成する。

【００６７】

ここで、ハッシュ関数について説明する。

【００６８】

ハッシュ関数Ｈとは、任意のビット長のディジタルデータＭから、一定のビット長となる出力ｈを生成する機能を持つ。この出力ｈは、ハッシュ値と呼ばれる（又は、ディジタル著名、メッセージダイジェスト、ディジタル指紋等とも呼ばれる）。通常、ハッシュ関数には、一方向性と衝突耐性とが要求される。一方向性とは、ハッシュ値ｈが与えられた際に、ｈ＝Ｈ（Ｍ）となるディジタルデータＭの算出が計算量的に困難であることを示す。又、衝突耐性とは、ディジタルデータＭが与えられた際に、Ｈ（Ｍ）＝Ｈ（Ｍ’）となるディジタルデータＭ’（Ｍ≠Ｍ’）の算出およびＨ（Ｍ）＝Ｈ（Ｍ’）且つＭ≠Ｍ’となるディジタルデータ

M、M'の算出が計算量的に困難であることを示す。ハッシュ関数には、ＭＤ－２、ＭＤ－４、ＭＤ－５、ＳＨＡ－１、ＲＩＰＥＭＤ－１２８、ＲＩＰＥＭＤ－１６０等の方式が知られている。第１の実施例では、ＭＤ－５方式を使用する例について説明する。尚、このＭＤ－５方式を用いて生成されるディジタル署名データのビット長は１２８ビットとなる。

【００６９】

ステップＳ４０７において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データとそれに対応するディジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【００７０】

尚、図４に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。これにより、ディジタル画像を撮像する毎にその画像に対応したディジタル署名データを生成することができる。

【００７１】

以上説明したように、第１の実施例では、高能率符号化されたディジタル画像データと画像入力装置１０の有する固有の秘密情報とを用いて所定の演算を行い、その演算結果をハッシュ関数演算することによってそのディジタル画像データのディジタル署名データを生成している。これにより、不正なユーザは秘密情報がわからない限り、ディジタル画像データからディジタル署名データを生成することはできない。又、ディジタル画像データに対する不正な処理（例えば、不正な合成、改竄）をディジタル署名データに反映させることもできない。又、ディジタル画像データと共に得られたディジタル署名データから元のデータ（即ち、ハッシュ関数演算する前のデータ）を知ることもできない。

【００７２】

このような構成により第１の実施例では、ディジタルデータの著作権を保護すると共に、そのディジタルデータに対する不正な処理を簡単な構成で、高速に検出することができる。又、上述のディジタル署名データを用いて、ある画像デー

タがどの画像入力装置にて撮像されたかを特定することもできる。

【００７３】

尚、第１の実施例では、上述の秘密情報を画像入力装置１０の製造時に設定された情報としたがそれに限るものではない。画像検証装置２０の秘密情報と共有できるものであれば、乱数発生回路２１４が所定のアルゴリズムに基づいて生成したビット列でもよい。

【００７４】

又、第１の実施例では、上述の所定の演算処理の一例として、ＪＰＥＧデータのバイトデータと秘密情報とを排他的論理和演算する構成について説明したがそれに限るものではない。高能率符号化されたディジタル画像データの少なくとも一部に秘密情報を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

【００７５】

又、第１の実施例では、高能率符号化後のディジタル画像データを記録媒体内に格納する前にディジタル署名データを生成する手順について説明したがそれに限るものではない。例えば、高能率符号化後のディジタル画像データを一度記録媒体内に格納した後、そのディジタル画像データを外部へ出力する前に上述の手順でディジタル署名データを生成するようにしてもよい。つまり、画像入力装置１０から外部へ出力される前に必ずディジタル署名データを生成する構成であれば、どのタイミングでディジタル署名データを生成してもよい。但し、ディジタル画像データを取り外し可能な記録媒体に記憶する場合には、上述の手順でディジタル署名データを生成する。

【００７６】

（第２の実施例）

第２の実施例では、第１の実施例に比べてより安全性の高いディジタル署名データを生成する手順について詳細に説明する。より具体的には、第１の実施例のハッシュ関数演算の際に、演算データをフィードバックし、撹乱するように構成する。

【００７７】

図６は、第２の実施例の処理手順を説明するフローチャートである。以下、図６に基づいて、ユーザの撮影指示後からディジタル署名データを生成するまでの手順について説明する。

【００７８】

ステップＳ６０１～Ｓ６０３の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。

【００７９】

ステップＳ６０４において、制御／演算部２０６（に含まれる乱数発生回路２１４）は、所定の情報（例えば、高能率符号化されたディジタル画像データのデータ量）を基にしてビット長ｍの乱数Ｒを生成する。この乱数Ｒが第２の実施例の秘密情報である。

【００８０】

次のステップＳ６０５～Ｓ６０６では、第２の実施例における所定の演算処理を説明する。

【００８１】

ステップＳ６０５において、制御／演算部２０６（に含まれる演算回路２１２）は、図７に示すように、１画像分のＪＰＥＧデータを所定の大きさ、例えば１２８ビット長のブロックＤｉ（ｉ＝１，２，３…Ｎ）に分割する。ここで、Ｄ１を最上位ブロックとする。ここで、ＪＰＥＧデータの総量が１２８の倍数にならない場合、１２８の倍数になるようにするパディングする。例えば、図７に示すように最後のブロックに“０００･･･０００”を付加することが考えられる。

【００８２】

ステップＳ６０６において、制御／演算部２０６（に含まれる演算回路２１２）は、上述の乱数Ｒと上述のＮ個のブロックとを用いて以下に示す手順の演算を行う。

【００８３】

まず、制御／演算部２０６は、図８に示すように、乱数Ｒのビット数を図７に示すブロックＤｉの個数Ｎと同じとなるように処理する。例えば、ｍ≧Ｎの場合

、最上位ビットからｎ（ｎ＝Ｎ）ビットまでのビット列を有効とし、それ以外のビット列を切り捨てる。又、ｍ＜Ｎの場合、不足分のデータとして“１１１…１１１”を付加する。

【００８４】

次に、制御／演算部２０６は、図９に示すように、各ブロックＤ１～ＤＮと各乱数Ｒ１～Ｒｎとで所定の演算を行う。具体的には、乱数ＲのビットＲｉとブロックＤｉの最下位ビットとの間で排他的論理和演算を行い、その演算をｉ＝１～ｎとなるまで繰り返し行う。

【００８５】

ここで、ステップＳ６０６の演算は、乱数ＲｉとブロックＤｉの最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロックＤｉの少なくとも一部に秘密情報（ビット長ｍの乱数Ｒの一部）を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

【００８６】

ステップＳ６０７において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ６０６の出力に対してハッシュ関数演算を施し、ディジタル署名データを生成する。尚、第２の実施例では、第１の実施例と同様に、ＭＤ－５方式のハッシュ関数を用いる。従って、ディジタル署名データのビット長は、１２８ビットとなる。

【００８７】

以下、ステップＳ６０７におけるハッシュ関数演算について説明する。

【００８８】

制御／演算部２０６は、後述する３つの動作モードの何れか１つ又はこれらの組み合わることによりハッシュ値ｈを求める。何れの演算方法においても、演算データを撹乱しながらハッシュ値を求めるため、より安全性の高いディジタル署名データを生成することができる。又、何れの演算方法においても、前の演算の結果が次の演算の結果に反映されるため、各演算単位毎にデータの正当性を検証することもできる。

【００８９】

①第１のモード

図１０を用いて説明する。図１０は、制御／演算部２０６の構成の一部を示す図である。

【００９０】

図１０において、演算回路２１２は、所定のビット単位でハッシュ関数演算を行うハッシュ関数演算回路１００１と、ハッシュ関数演算回路１００１の出力ｈの一部を記憶するレジスタ１００２と、ステップＳ６０６の処理を実現する演算回路１００３と、演算回路１００３の出力とレジスタ１００２の出力とを排他的論理和演算する演算回路１００４とから構成されている。

【００９１】

ハッシュ関数演算回路１００１の出力である１２８ビットのハッシュ値ｈの一部は、レジスタ１００２に入力される。レジスタ１００２には、例えば、ハッシュ値ｈの上位６４ビットが一時的に格納される。

【００９２】

レジスタ１００２に格納された６４ビットデータは、次の演算対象（ＪＰＥＧデータの一部）と排他的論理和演算され、その演算結果はハッシュ関数演算回路１００１に供給される。

【００９３】

最終的に、１ＪＰＥＧデータを複数のブロック単位毎に順次ハッシュ関数演算した結果が、１２８ビットのディジタル署名データとして出力される。

【００９４】

ここで、最初の演算では、レジスタ１００２に初期値を格納しておく必要がある。その初期値は、例えば図１３に示すように、乱数Ｒの下位６４ビットを用いることができる。

【００９５】

尚、ブロックＤｉの大きさが６４の倍数とならない場合には、例えば後述の第３のモードと組合せて余りのビット列を演算するように構成してもよい。

【００９６】

②第２のモード

図１１を用いて説明する。図１１は、制御／演算部２０６の構成の一部を示す図である。

【００９７】

図１１において、演算回路２１２は、所定のビット単位でハッシュ関数演算を行うハッシュ関数演算回路１１０１と、ハッシュ関数演算回路１１０１に必要な入力値を供給するレジスタ１１０２と、ハッシュ関数演算回路１１０１の出力ｈを選択的に出力するセレクタ１１０３と、ステップＳ６０６の処理を実現する演算回路１１０４と、演算回路１１０４の出力とセレクタ１１０３の出力とを排他的論理和演算する演算回路１１０５とから構成されている。

【００９８】

ハッシュ関数演算回路１１０１は、乱数発生回路２１４にて生成された秘密情報を初期値とするレジスタ１１０２の値を順次ハッシュ関数演算する。

【００９９】

ハッシュ関数演算回路１１０１の出力である１２８ビットのハッシュ値ｈは、セレクタ１１０３に入力される。セレクタ１１０３は、１２８ビットのハッシュ値ｈの内、例えば下位Ｋビットをシフトして出力する。このＫビットは、次にハッシュ関数演算されるデータとしてレジスタ１１０２に格納される。

【０１００】

又、セレクタ１１０３から出力されたＫビットは、演算回路１１０４の出力の一部と排他的論理和演算され、その結果が１２８ビットのディジタル署名データとなる。

【０１０１】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図１３に示すように、上述の乱数Ｒの下位６４ビットを用いることができる。

【０１０２】

③第３のモード

図１２を用いて説明する。図１２は、制御／演算部２０６の構成の一部を示す

図である。

【０１０３】

図１２において、演算回路２１２は、所定のビット単位でハッシュ関数演算を行うハッシュ関数演算回路１２０１と、ハッシュ関数演算回路１２０１に必要な入力値を供給するレジスタ１２０２と、ハッシュ関数演算回路１２０１の出力ｈを選択的に出力するセレクタ１２０３と、ステップＳ６０６の処理を実現する演算回路１２０４と、演算回路１２０４の出力とセレクタ１２０３の出力とを排他的論理和演算する演算回路１２０５とから構成されている。

【０１０４】

ハッシュ関数演算回路１２０１は、乱数発生回路２１４にて生成された秘密情報を初期値とするレジスタ１１０２の値を順次ハッシュ関数演算する。

【０１０５】

ハッシュ関数演算回路１２０１の出力である１２８ビットのハッシュ値ｈは、セレクタ１２０３に入力される。セレクタ１２０３は、１２８ビットのハッシュ値ｈの内、例えば下位Ｋビットをシフトして出力する。このＫビットは、次の演算対象（ＪＰＥＧデータの一部）と排他的論理和演算され、その演算結果の一部は再びレジスタ１２０２に格納される。

【０１０６】

最終的に、１ＪＰＥＧデータを複数のブロック単位毎に順次ハッシュ関数演算した結果が、１２８ビットのディジタル署名データとして出力される。

【０１０７】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図１３に示すように、上述の乱数Ｒの下位６４ビットを用いることができる。

【０１０８】

ステップＳ６０８において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データとそれに対応するディジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【０１０９】

尚、図６に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納

されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。

【０１１０】

以上のように第２の実施例では、ある長さの乱数を生成し、その乱数と高能率符号化されたディジタル画像データとを用いて所定の演算処理を行い、その演算結果をハッシュ関数演算してディジタル署名データを生成している。このような構成により第２の実施例では、ディジタルデータの著作権を保護すると共に、そのディジタルデータに対する不正な処理を簡単な構成で、高速に検出することができる。

【０１１１】

又、第２の実施例では、ハッシュ関数演算を上述の動作モードの１つまたは複数を組み合わせて実現することにより、第１の実施例に比べてより安全性の高いディジタル署名データ生成アルゴリズムを提供することができる。

【０１１２】

又、第２の実施例では、上述のディジタル署名データを用いて、ある画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【０１１３】

（第３の実施例）

第１、第２の実施例では、ハッシュ関数を用いてディジタル署名データを生成する手順について説明した。

【０１１４】

第３の実施例では、ハッシュ関数ではなく共通鍵暗号処理を用いてディジタル署名データを生成する手順について詳細に説明する。

【０１１５】

図１４は、第３の実施例の処理手順を説明するフローチャートである。以下、図１４に基づいて、ユーザの撮影指示後からディジタル署名データを生成するまでの手順について説明する。

【０１１６】

ステップＳ１４０１～Ｓ１４０３の処理は、上述の第１の実施例のステップＳ

４０１～Ｓ４０３と同様の処理としてその説明を省略する。

【０１１７】

ステップＳ１４０４において、制御／演算部２０６は、画像入力装置１０の持つ固有の秘密情報をメモリ２１３から読み出す。第３の実施例では、“１１１１…１１１１”（１２８ビット）を秘密情報とする。尚、この秘密情報は、一般に公開されず且つ画像検証装置２０の持つ固有の秘密情報と共有できるものであればいかなるデータであってもよい。

【０１１８】

ステップＳ１４０５において、制御／演算部２０６（に含まれる演算回路２１２）は、作業用メモリ２０２に保持されたＪＰＥＧデータを共通鍵暗号方式に基づいて暗号化する。

【０１１９】

ここで、共通鍵暗号方式には現在様々なものが提案されているが、例えば第３の実施例ではＤＥＳ方式を用いる。ＤＥＳ方式を使用する場合、暗号鍵のビット長は５６ビットであるので、図１５に示すように秘密情報の上位５６ビットを暗号鍵とすることが考えられる。ここで、この暗号鍵のビット長は、使用する共通鍵暗号方式の種類によって異なるものである。従って、FEAL-nX,MITSY,IDEAを使用する場合、暗号鍵は１２８ビットであるので秘密情報の上位１２８ビットを暗号鍵としてもよい。又、FEAL-n,MULTI2を使用する場合、暗号鍵は６４ビットであるので秘密情報の上位６４ビットを暗号鍵としてもよい。

【０１２０】

以下、ステップＳ１４０５における暗号化処理について説明する。

【０１２１】

制御／演算部２０６は、後述する３つの動作モード（即ち、ＣＢＣモード、ＣＦＢモード、ＯＦＢモード）の何れか１つ又はこれらの組み合わることによりＪＰＥＧデータを上述の暗号鍵で暗号化する。何れの動作モードにおいても、入力データをデータ量に関わらず暗号化することができ、且つ入力データを撹乱しながら暗号化することができるのでより安全性の高い暗号化処理を実現できる。

【０１２２】

①ＣＢＣ（Cipher Block Chaining）モード

図１６を用いて説明する。図１６は、制御／演算部２０６の一部（即ち、演算回路２１２）を示す図である。

【０１２３】

図１６において、演算回路２１２は、６４ビット単位で暗号化を行う暗号化回路１６０１と、暗号化回路１６０１の出力を一時的に保持するレジスタ１６０２と、ＪＰＥＧデータとレジスタ１６０２の出力とを排他的論理和演算する演算回路１６０３とから構成されている。

【０１２４】

暗号化回路１６０１は、６４ビット単位で暗号化を行う。従って、暗号化回路１６０１は、ＪＰＥＧデータを６４ビットからなるブロック毎に暗号化する。暗号化回路１６０１の出力はレジスタ１６０２に一時的に格納される。レジスタ１６０２に格納された６４ビットデータは、次のブロックと排他的論理和演算され、その演算結果は暗号化回路１６０１に供給される。最終的に、全てのブロックを暗号化した結果が暗号データとして出力される。

【０１２５】

ここで、最初のブロックの暗号化では、レジスタ１６０２に初期値を格納しておく必要がある。その初期値は、例えばＩＶ（Initial Vector）と呼ばれる初期値を使用する。このＩＶは、暗号化処理と復号処理において同じ値を供給する必要がある。又、例えば、図１５に示すように、秘密情報の下位６４ビットを用いることもできる。

【０１２６】

尚、ブロックの大きさが６４の倍数とならない場合には、例えば後述のＯＦＢモードと組合せて余りのビット列を暗号化するように構成してもよい。

【０１２７】

②ＣＦＢ（Cipher Feedback）モード

図１７を用いて説明する。図１７は、制御／演算部２０６の一部（即ち、演算回路２１２）を示す図である。ＣＦＢモードでは、暗号化側と復号側とで同じ長

さのビット列を暗号化が可能な場合に利用される。

【０１２８】

図１７において、演算回路２１２は、６４ビット単位で暗号化を行う暗号化回路１７０１と、暗号化回路１７０１に必要な入力値を供給するレジスタ１７０２と、暗号化回路１７０１の出力を選択的に出力するセレクタ１７０３と、ＪＰＥＧデータとセレクタ１７０３の出力とを排他的論理和演算する演算回路１７０４とから構成されている。

【０１２９】

暗号化回路１７０１は、６４ビット単位で暗号化を行う。従って、暗号化回路１７０１は、レジスタ１７０２に格納された６４ビットデータを順次暗号化する。暗号化回路１７０１の出力は、セレクタ１７０３に入力される。セレクタ１７０３は、例えば下位Ｋビットをシフトして出力する。このＫビットは、次に暗号化されるデータとしてレジスタ１７０２に格納される。セレクタ１７０３から出力されたＫビットは、ＪＰＥＧデータの一部（６４ビットのブロック）と排他的論理和演算され、その結果が暗号データとなる。

【０１３０】

ここで、最初の暗号化に必要な初期値は、例えば図１５に示しように、上述の秘密情報の下位６４ビットを用いることができる。

【０１３１】

③ＯＦＢ（Output Feedback）モード

図１８を用いて説明する。図１８は、制御／演算部２０６の一部（即ち、演算回路２１２）を示す図である。ＯＦＢモードは、ＣＦＢモードと同様に、暗号化側と復号側とで同じ長さのビット列を暗号化が可能な場合に利用される。

【０１３２】

図１８において、演算回路２１２は、６４ビット単位で暗号化を行う暗号化回路１８０１と、暗号化回路１８０１に必要な入力値を供給するレジスタ１８０２と、暗号化回路１８０１の出力を選択的に出力するセレクタ１８０３と、ＪＰＥＧデータとセレクタ１８０３の出力とを排他的論理和演算する演算回路１８０４とから構成されている。

【０１３３】

暗号化回路１８０１は、６４ビット単位で暗号化を行う。従って、暗号化回路１８０１は、レジスタ１８０２に格納された６４ビットデータを順次暗号化する。暗号化回路１８０１の出力は、セレクタ１８０３に入力される。セレクタ１８０３は、例えば下位Ｋビットをシフトして出力する。セレクタ１８０３から出力されたＫビットは、ＪＰＥＧデータの一部（６４ビットのブロック）と排他的論理和演算され、その結果が暗号データとなる。ここで、暗号データの一部（Ｋビット）は、再びレジスタ１８０２に格納される。

【０１３４】

ここで、最初のハッシュ関数演算に必要な初期値は、例えば図１５に示しように、上述の秘密情報の下位６４ビットを用いることができる。

【０１３５】

ステップＳ１４０６において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ１４０５にて生成された暗号データから特定のビット列をディジタル署名データとして抽出する。例えば、上述の暗号データの下位１２８ビットをディジタル署名データとすることができる。

【０１３６】

ステップＳ１４０７において、記録再生部２０３は、制御／演算部２０６（に含まれる演算回路２１２）にて生成されたディジタル署名データとそれに対応するディジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【０１３７】

尚、図１４に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。

【０１３８】

以上のように第３の実施例では、画像入力装置１０と画像検証装置２０とで共有される秘密情報の一部からなる暗号鍵を用いて、高能率符号化されたディジタル画像データを暗号化し、その結果生成された暗号データの一部をディジタル署名データとする構成について説明した。このような構成により第３の実施例では

、ディジタルデータの著作権を保護すると共に、第１の実施例に比べてより安全性の高いディジタル署名データ生成アルゴリズムを提供することができる。

【０１３９】

又、第３の実施例では、上述のディジタル署名データを用いて、あるディジタル画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【０１４０】

尚、第３の実施例では、秘密情報を“１１１１…１１１１”（１２８ビット）としたがこれに限るものではない。例えば、乱数発生回路２１４が所定のアルゴリズムに基づいて発生させた乱数とすることも可能である。但し、この秘密情報は画像検証装置２０と共有される。

【０１４１】

（第４の実施例）

第３の実施例では、ハッシュ関数演算ではなく共通鍵暗号演算を用いてディジタル署名データを生成する手順について説明した。

【０１４２】

第４の実施例では、共通鍵暗号演算の前に所定の演算処理（例えば、ビット挿入を含む逆演算可能な演算処理）を行い、その演算結果を暗号化し、その暗号結果からディジタル署名データを生成する手順について説明する。

【０１４３】

図１９は、第４の実施例の処理手順を説明するフローチャートである。以下、図１９に基づいて、ユーザの撮影指示後からディジタル署名データを生成するまでの手順について説明する。

【０１４４】

ステップＳ１９０１～Ｓ１９０３の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。

【０１４５】

ステップＳ１９０４～Ｓ１９０６の処理は、上述の第２の実施例のステップＳ６０４～Ｓ６０６と同様の処理（即ち、秘密情報である乱数ＲのビットＲｉとＪＰＥＧデータのブロックＤｉとを用いた排他的論理和演算）としてその説明を省

略する。

【０１４６】

ここで、ステップＳ１９０６の演算は、上述のステップＳ６０６と同様に、乱数Ｒｉとブロック Ｄｉの最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロックＤｉの少なくとも一部に秘密情報（ビット長ｍの乱数Ｒの一部）を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

【０１４７】

ステップＳ１９０７において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ１９０６の出力に対して共通鍵暗号化方式に従った暗号化処理を施す。ここで、制御／演算部２０６は、第３の実施例と同様に、ＤＥＳ方式を利用するものとし、その暗号化処理に必要な暗号鍵は、ステップＳ１９０４で生成した秘密情報（即ち、乱数Ｒ）の上位５６ビットとする（図２０参照）。

【０１４８】

以下、ステップＳ１９０７における暗号化処理について説明する。

【０１４９】

制御／演算部２０６は、上述した３つの動作モード（即ち、ＣＢＣモード、ＣＦＢモード、ＯＦＢモード）の何れか１つ又はこれらの組み合わることにより、乱数ＲのビットＲｉとＪＰＥＧデータのブロックＤｉとの排他的論理和演算の結果を上述の暗号鍵を用いて順次暗号化する。何れの動作モードにおいても、入力データをデータ量に関わらず暗号化することができ、且つ入力データを撹乱しながら暗号化することができるのでより安全性の高い暗号化処理を実現できる。

【０１５０】

尚、これらの動作モードにおいて、最初のブロックの暗号化では、上述のように初期値が必要であるが、例えばその初期値を図２０に示すように、秘密情報（即ち、乱数Ｒ）の下位６４ビットとすることができる。

【０１５１】

又、ＣＢＣモードにおいて、ブロックＤｉの大きさが６４の倍数とならない場合には、例えば後述のＯＦＢモードと組合せて余りのビット列を暗号化するよう

に構成してもよい。

【０１５２】

ステップＳ１９０８において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ１９０７にて生成された暗号データから特定のビット列をディジタル署名データとして抽出する。例えば、上述の暗号データの下位１２８ビットをディジタル署名データとすることができる。

【０１５３】

ステップＳ１９０９において、記録再生部２０３は、制御／演算部２０６（に含まれる演算回路２１２）にて生成されたディジタル署名データとそれに対応するディジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【０１５４】

尚、図１９に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。

【０１５５】

以上のように第４の実施例では、ある長さの乱数を発生させ、その乱数と高能率符号化されたディジタル画像データとをあらかじめ決められた規則に従った演算を行い、その演算結果を共通鍵暗号方式により暗号化し、その結果得られた暗号データの一部をディジタル署名データとしている。このような構成により第４の実施例では、ディジタルデータの著作権を保護すると共に、第１、第２の実施例に比べてより安全性の高いディジタル署名データ生成アルゴリズムを提供することができる。

【０１５６】

又、第４の実施例では、共通鍵暗号化方式による暗号化処理を上述の動作モードの１つまたは複数を組み合わせて実現することにより、第１、第２の実施例に比べてより安全性の高いディジタル署名データ生成アルゴリズムを提供することができる。

【０１５７】

又、第４の実施例では、上述のディジタル署名データを用いて、あるディジタ

ル画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【０１５８】

（第５の実施例）

第１～第４の実施例では、画像入力装置１０が、画像入力装置１０自体の持つ固有の秘密情報に基づいてディジタル署名データを生成する構成について説明した。このような構成により第１～第４の実施例では、ディジタル署名データを用いて、ある画像データがどの画像入力装置にて撮像されたものであるかを特定することができる。

【０１５９】

これに対して、第５の実施例では、外部装置（例えば，ＩＣカード等）を画像入力装置１０に接続し、この外部装置の持つ固有の秘密情報に基づいてディジタル署名データを生成する構成について説明する。ここで、外部機器の持つ秘密情報は、例えば、画像入力装置１０を識別するためのＩＤ情報、画像入力装置１０を使用するユーザを識別するためのＩＤ情報とすることができる。このように構成することにより第５の実施例では、ディジタル署名データを用いて、ある画像データがどの外部機器を使用して撮像されたものか、或いはどのユーザによって撮像されたものであるかを特定することができる。

【０１６０】

図２１は、第５の実施例の処理手順を説明するフローチャートである。以下、図２１に基づいて、外部装置の接続からディジタル署名データの生成までの手順について説明する。

【０１６１】

ステップＳ２１０１において、画像入力装置１０の制御/演算処理部２０６は、外部Ｉ／Ｆ部２０５に外部装置４０が接続されているか否かを検出する。

【０１６２】

ステップＳ２１０２において、画像入力装置１０の制御/演算処理部２０６及び外部装置４０の制御/演算処理部３０６とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

【０１６３】

ここで、図２２を用いて画像入力装置１０と外部装置４０との相互認証処理について説明する。

【０１６４】

画像入力装置１０は、乱数発生回路２１４を用いて認証用の乱数ａを発生させ、その乱数ａを外部Ｉ／Ｆ部２０５を介して外部装置４０に送信する。

【０１６５】

次に外部装置４０の暗号化回路４３は、認証用の暗号鍵を用いて乱数ａをＡに変換し、その暗号データＡを外部Ｉ／Ｆ部４１を介して画像入力装置１０へ送信する。

【０１６６】

又、画像入力装置１０の暗号化回路２２０１は、乱数ａを認証用の暗号鍵を用いてＡ’に変換する。比較回路２２０２は、その暗号データＡ’を外部装置４０から送信された暗号データＡと比較し、それらが一致すれば外部装置４０を認証する。

【０１６７】

同様にして、外部装置４０は、乱数発生回路４２を用いて認証用の乱数ｂを発生させ、その乱数ｂを外部Ｉ／Ｆ部２０５を介して画像入力装置１０に送信する。

【０１６８】

次に画像入力装置１０の暗号化回路２２０１は、認証用の暗号鍵を用いて乱数ｂをＢに変換し、その暗号データＢを外部Ｉ／Ｆ部２０５を介して外部装置４０へ送信する。

【０１６９】

又、外部装置４０の暗号化回路４３は、乱数ｂを認証用の暗号鍵を用いてＢ’に変換する。比較回路４４は、その暗号データＢ’を画像入力装置１０から送信された暗号データＢと比較し、それらが一致すれば画像入力装置１０を認証する。

【０１７０】

双方が正常に認証された場合、外部装置４０は、メモリ４５に格納された秘密情報を外部Ｉ／Ｆ部４１を介して画像入力装置１０に送信する。

【０１７１】

ステップＳ２１０３～Ｓ２１０５の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。

【０１７２】

ステップＳ２１０６において、制御／演算部２０６は、外部Ｉ／Ｆ部２０５を介して入力された外部装置４０の持つ固有の秘密情報をメモリ２１３に格納し、ディジタル署名データの生成に必要な秘密情報として管理する。

【０１７３】

ステップＳ２１０７において、制御／演算部２０６（に含まれる演算回路２１２）は、上述の秘密情報と例えばＪＰＥＧ方式で高能率符号化されたディジタル画像データ（以下、ＪＰＥＧデータと称する）とを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路２１２は、第１の実施例のステップＳ４０５と同様の演算処理を行う。

【０１７４】

ステップＳ２１０８において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ２１０７の演算結果をハッシュ関数演算し、その結果からディジタル署名データを生成する。ここで、演算回路２１２は、第１の実施例のステップＳ４０６と同様の演算処理を行う。

【０１７５】

ステップＳ２１０９において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データとそれに対応するディジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【０１７６】

尚、図２１に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デ

ィジタル画像を撮像する毎にその画像に対応したディジタル署名データを生成することができる。

【０１７７】

以上説明したように、第５の実施例では、画像入力装置１０の高能率符号化されたディジタル画像データと画像入力装置１０と接続された外部装置４０の有する秘密情報とを用いて所定の演算を行い、その演算結果をハッシュ関数演算することによってそのディジタル画像データのディジタル署名データを生成している。これにより、不正なユーザはこの秘密情報がわからない限り、ディジタル画像データからディジタル署名データを生成することはできない。又、ディジタル画像データに対する不正な処理（例えば、不正な合成、改竄）をディジタル署名データに反映させることもできない。又、ディジタル画像データと共に得られたディジタル署名データから元のデータ（即ち、ハッシュ関数演算する前のデータ）を知ることもできない。

【０１７８】

このような構成により第５の実施例では、ディジタルデータの著作権を保護すると共に、そのディジタルデータに対する不正な処理を検出するための署名データを簡単な構成で、高速に生成することができる。又、上述のディジタル署名データを用いて、ある画像データがどの外部機器或いはどのユーザにて撮像されたかを特定することもできる。

【０１７９】

尚、第５の実施例では、ディジタル署名データを生成するための演算処理を第１の実施例と同様の演算処理としたがそれに限るものではない。上述の第２～第４の実施例と同様の演算処理を適用することも可能である。

【０１８０】

（第６の実施例）

第５の実施例では、画像入力装置１０に外部装置４０を接続し、この外部装置４０の持つ固有の秘密情報に基づいてディジタル署名データを生成する構成について説明した。

【０１８１】

これに対して、第６の実施例では、画像入力装置１０を外部装置４０に接続し、この外部装置４０の持つ固有の秘密情報と画像入力装置１０の持つ固有の秘密情報とに基づいてディジタル署名データを生成する構成について説明する。このように構成することにより第６の実施例では、ディジタル署名データを用いて、ある画像データがどの外部機器と接続されたどの画像入力装置によって撮像されたものか、或いはどのユーザが使用するどの画像入力装置によって撮像されたものであるかを特定することができる。

【０１８２】

以下、図２１を用いて第６の実施例の処理手順を説明する。

【０１８３】

ステップＳ２１０１において、画像入力装置１０の制御/演算処理部２０６は、外部Ｉ／Ｆ部２０５に外部装置４０が接続されているか否かを検出する。

【０１８４】

ステップＳ２１０２において、画像入力装置１０の制御/演算処理部２０６及び外部装置４０の制御/演算処理部３０６とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。相互認証処理の一例を図２２に示す。

【０１８５】

ステップＳ２１０３～Ｓ２１０５の処理は、上述の第１の実施例のステップＳ４０１～Ｓ４０３と同様の処理としてその説明を省略する。

【０１８６】

ステップＳ２１０６において、制御／演算部２０６は、画像入力装置１０の持つ固有の秘密情報をメモリ２１３から読み出し、外部装置４０の持つ固有の秘密情報を外部Ｉ／Ｆ部２０５を介して入力する。そして、これらの秘密情報を結合させ、新しい秘密情報を生成する。

【０１８７】

ここで、画像入力装置１０の秘密情報を例えば“１１１１”とし、外部装置４０の秘密情報を例えば“００００”とすると、新たに生成される秘密情報は、例えば“１１１１０００”となる。尚、第６の実施例では、２つの秘密情報を単

に結合することにより新たな秘密情報を生成したが、これら２つの秘密情報のみに基づいて生成されるのであれば、どのような演算であってもよい。又、これら２つの秘密情報は、画像検証装置２０の持つ固有の秘密情報と共有できるものであればいかなるデータであってもよい。

【０１８８】

ステップＳ２１０７において、制御／演算部２０６（に含まれる演算回路２１２）は、上述の秘密情報と例えばＪＰＥＧ方式で高能率符号化されたディジタル画像データ（以下、ＪＰＥＧデータと称する）とを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路２１２は、第１の実施例のステップＳ４０５と同様の演算処理を行う。

【０１８９】

ステップＳ２１０８において、制御／演算部２０６（に含まれる演算回路２１２）は、ステップＳ２１０７の演算結果をハッシュ関数演算し、その結果からディジタル署名データを生成する。ここで、演算回路２１２は、第１の実施例のステップＳ４０６と同様の演算処理を行う。

【０１９０】

ステップＳ２１０９において、記録再生部２０３は、制御／演算部２０６にて生成されたディジタル署名データとそれに対応するディジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【０１９１】

尚、図２１に示す一連の処理手順を制御するプログラムは、ＲＯＭ２０７に格納されている。このプログラムは、制御／演算部２０６（に含まれる制御回路２１０）によって読み出され、ユーザの撮像指示毎に起動される。これにより、ディジタル画像を撮像する毎にその画像に対応したディジタル署名データを生成することができる。

【０１９２】

以上説明したように、第６の実施例では、画像入力装置１０の高能率符号化されたディジタル画像データと、画像入力装置１０の有する秘密情報と、外部装置４０の有する秘密情報とを用いて所定の演算を行い、その演算結果をハッシュ関

数演算することによってそのディジタル画像データのディジタル署名データを生成している。

【０１９３】

このような構成により第６の実施例では、ディジタルデータの著作権を保護すると共に、そのディジタルデータに対する不正な処理を検出するための署名データを簡単な構成で、高速に生成することができる。又、上述のディジタル署名データを用いて、ある画像データがどの外部機器と接続された画像入力装置或いはどのユーザによって使用された画像入力装置にて撮像されたかを特定することもできる。

【０１９４】

尚、第６の実施例では、ディジタル署名データを生成するための演算処理を第１の実施例と同様の演算処理としたがそれに限るものではない。上述の第２～第４の実施例と同様の演算処理を適用することも可能である。

【０１９５】

（第７の実施例）

第７の実施例では、画像検証装置２０が、第１の実施例に基づいて生成されたディジタル署名データを用いて、ＪＰＥＧデータの正当性を確認する構成について説明する。

【０１９６】

具体的に、画像検証装置２０は、外部入力されたＪＰＥＧデータと、画像入力装置１０と画像検証装置２０とで共有する秘密情報とに基づいて所定の演算を行い、その演算結果と該ＪＰＥＧデータとセットで入力されたディジタル署名データとを比較し、その比較結果に基づいて該ＪＰＥＧデータの正当性を検証する。

【０１９７】

図２３は、第７の実施例の処理手順の一例を説明するフローチャートである。以下、図２３に基づいて、ディジタル画像データの入力からその検証までの手順について説明する。

【０１９８】

ステップＳ２３０１において、外部Ｉ／Ｆ部３０１は、画像入力装置１０から

送信された１画像分の高能率符号化データ（例えば、ＪＰＥＧ方式で圧縮符号化されたＪＰＥＧデータ）とそれに対応するディジタル署名データとを入力し、それらを画像検証装置２０内の記録媒体（例えば、作業用メモリ３０２）に格納する。

【０１９９】

ステップＳ２３０２において、操作部３０６は、所望のＪＰＥＧデータを選択し、そのＪＰＥＧデータの正当性を検証するか否かを選択する。検証が指示された場合、制御／演算部２０６はステップＳ２３０３を実行する。

【０２００】

ステップＳ２３０３において、制御／演算部３０３は、メモリ３１３から秘密情報を読み出す。ここで、この秘密情報は、第１の実施例の画像入力装置１０と本実施例の画像検証装置２０とで共有している秘密情報である。従って、本実施例の秘密情報は、第１の実施例と同様に“１１１１１１１１”とすることができる。尚、この秘密情報は、読み出し専用の記録媒体等の中に保存され、外部からその情報を入手できないように管理されている。

【０２０１】

ステップＳ２３０４において、制御／演算部３０３（に含まれる演算回路３１２）は、上述の秘密情報と選択されたＪＰＥＧデータとを用いて、第１の実施例のステップＳ４０５と同様の演算を行う。つまり、ＪＰＥＧデータの最上位バイトと秘密情報とをビット毎に排他的論理和演算する。

【０２０２】

ステップＳ２３０５において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２３０４の演算結果に対してハッシュ関数演算を行う。ここでは、第１の実施例と同様のハッシュ関数が使用される。

【０２０３】

ステップＳ２３０６において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２３０５の演算結果と、選択されたＪＰＥＧデータとセットで入力されたディジタル署名データを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合

には、ＪＰＥＧデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【０２０４】

ステップＳ２３０７において、表示部３０４は、ステップＳ２３０５の比較結果が一致した場合、選択されたＪＰＥＧデータが正常で、不正な処理の施されていないことを示す表示画像或いはメッセージを表示する。又、この比較結果が一致しなかった場合、不正な処理を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２０５】

尚、図２３に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２０６】

以上の手順により、選択されたＪＰＥＧデータの正当性を確認した場合、ユーザは、操作部３０６を操作し、該ＪＰＥＧデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路３１０は各処理回路を制御し、該ＪＰＥＧデータを廃棄することもできる。

【０２０７】

以上説明したように、第７の実施例では、第１の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【０２０８】

（第８の実施例）

第８の実施例では、画像検証装置２０が、第２の実施例に基づいて生成されたディジタル署名データを用いて、ＪＰＥＧデータの正当性を確認する構成について説明する。

【０２０９】

図２４は、第８の実施例の処理手順の一例を説明するフローチャートである。

以下、図２４に基づいて、ディジタル画像データの入力からその検証までの手順について説明する。

【０２１０】

ステップＳ２４０１、Ｓ２４０２の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。

【０２１１】

ステップＳ２４０３において、制御／演算部３０３（に含まれる乱数発生回路）は、選択されたＪＰＥＧデータのデータ量を基にしてビット長ｍの乱数Ｒ（即ち、秘密情報）を発生させる。乱数Ｒを発生されるためのプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、第２の実施例の画像入力装置１０の保持するプログラムと同様であり、乱数Ｒは、第２の実施例の乱数Ｒと同様である。尚、このプログラム及び乱数Ｒは、外部からその情報を入手できないように管理されている。

【０２１２】

ステップＳ２４０４において、制御／演算部３０３（に含まれる演算回路３１２）は、図７に示すように、選択されたＪＰＥＧデータを１２８ビットのブロックＤｉ（ｉ＝１～ｎ）に分割し、１ブロックのデータ量が１２８ビットにならない分については“０００…０００”をパディングする。尚、ステップＳ２４０４の処理は、第２の実施例のステップＳ６０５と同様の処理である。

【０２１３】

ステップＳ２４０５において、制御／演算部３０３（に含まれる演算回路３１２）は、上述の乱数Ｒと上述のＮ個のブロックとを用いて第２の実施例のステップＳ６０６と同様の演算処理を行う。つまり、乱数ＲのビットＲｉとブロックＤｉの最下位ビットとの間の排他的論理和演算を、ｉ＝１～ｎとなるまで繰り返す。

【０２１４】

ステップＳ２４０６において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２４０５の演算結果に対してハッシュ関数演算を行う。ここでは、第２の実施例と同様のハッシュ関数が使用される。

【０２１５】

ステップＳ２４０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２４０６の演算結果と、選択されたＪＰＥＧデータとセットで入力されたディジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【０２１６】

ステップＳ２４０８において、表示部３０４は、ステップＳ２４０７の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２１７】

尚、図２４に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２１８】

以上の手順により、選択されたＪＰＥＧデータの正当性を確認した場合、ユーザは、操作部３０６を操作し、該ＪＰＥＧデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路３１０は各処理回路を制御し、該ＪＰＥＧデータを廃棄することもできる。

【０２１９】

以上説明したように、第８の実施例では、第２の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【０２２０】

（第９の実施例）

第９の実施例では、画像検証装置２０が、第３の実施例に基づいて生成されたディジタル署名データを用いて、ＪＰＥＧデータの正当性を確認する構成につい

て説明する。

【０２２１】

図２５は、第９の実施例の処理手順の一例を説明するフローチャートである。以下、図２５に基づいて、ディジタル画像データの入力からその検証までの手順について説明する。

【０２２２】

ステップＳ２５０１、Ｓ２５０２の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。

【０２２３】

ステップＳ２５０３において、制御／演算部３０３は、メモリ３１３から秘密情報を読み出す。ここで、この秘密情報は、第３の実施例の画像入力装置１０と本実施例の画像検証装置２０とで共有している秘密情報である。従って、本実施例の秘密情報は、第３の実施例と同様に“１１１１１１１１”とすることができる。尚、この秘密情報は、読み出し専用の記録媒体等の中に保存され、外部からその情報を入手できないように管理されている。

【０２２４】

ステップＳ２５０４において、制御／演算部３０３（に含まれる演算回路３１２）は、第３の実施例のステップＳ１４０５と同様に、選択されたＪＰＥＧデータを共通鍵暗号方式に基づいて暗号化する。ここで、ＪＰＥＧデータの暗号化使用される関数は、第３の実施例と同様の関数である。例えば、上述のＣＢＣモードとＯＦＢモードとを組み合わせて使用する場合、ＣＢＣモードを用いて入力データを６４ビット単位に暗号化し、余りのデータをＯＦＢモードにて暗号化する。

【０２２５】

ステップＳ２５０５において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２５０４にて生成された暗号データから特定のビット列を抽出する。例えば、第３の実施例と同様に、上述の暗号データの下位１２８ビットを抽出する。

【０２２６】

ステップＳ２５０６において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２５０５の抽出結果と、選択されたＪＰＥＧデータとセットで入力されたディジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【０２２７】

ステップＳ２５０７において、表示部３０４は、ステップＳ２５０６の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２２８】

尚、図２５に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２２９】

以上の手順により、選択されたＪＰＥＧデータの正当性を確認した場合、ユーザは、操作部３０６を操作し、該ＪＰＥＧデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路３１０は各処理回路を制御し、該ＪＰＥＧデータを廃棄することもできる。

【０２３０】

以上説明したように、第９の実施例では、第３の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【０２３１】

（第１０の実施例）

第１０の実施例では、画像検証装置２０が、第４の実施例に基づいて生成されたディジタル署名データを用いて、ＪＰＥＧデータの正当性を確認する構成につ

いて説明する。

【０２３２】

図２６は、第１０の実施例の処理手順の一例を説明するフローチャートである。以下、図２６に基づいて、ディジタル画像データの入力からその検証までの手順について説明する。

【０２３３】

ステップＳ２６０１、Ｓ２６０２の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。

【０２３４】

ステップＳ２６０３～Ｓ２６０５の処理は、上述の第８の実施例のステップＳ２４０３～Ｓ２４０５と同様の処理としてその説明を省略する。

【０２３５】

ステップＳ２６０６において、制御／演算部３０３（に含まれる演算回路３１２）は、第４の実施例のステップＳ１９０７と同様に、選択されたＪＰＥＧデータを共通鍵暗号方式に基づいて暗号化する。ここで、ＪＰＥＧデータの暗号化使用される関数は、第４の実施例と同様の関数である。

【０２３６】

ステップＳ２６０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２６０６にて生成された暗号データから特定のビット列を抽出する。例えば、第３の実施例と同様に、上述の暗号データの下位１２８ビットを抽出する。

【０２３７】

ステップＳ２６０８において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２６０７の抽出結果と、選択されたＪＰＥＧデータとセットで入力されたディジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【０２３８】

ステップＳ２６０９において、表示部３０４は、ステップＳ２６０８の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２３９】

尚、図２６に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２４０】

以上の手順により、選択されたＪＰＥＧデータの正当性を確認した場合、ユーザは、操作部３０６を操作し、該ＪＰＥＧデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路３１０は各処理回路を制御し、該ＪＰＥＧデータを廃棄することもできる。

【０２４１】

以上説明したように、第１０の実施例では、第４の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【０２４２】

（第１１の実施例）

第１１の実施例では、画像検証装置２０が、第５の実施例に基づいて生成されたディジタル署名データを用いて、ＪＰＥＧデータの正当性を確認する構成について説明する。

【０２４３】

図２７は、第１０の実施例の処理手順の一例を説明するフローチャートである。以下、図２７に基づいて、ディジタル画像データの入力からその検証までの手順について説明する。

【０２４４】

ステップＳ２７０１において、画像検証装置２０の制御/演算処理部３０３は

、外部Ｉ／Ｆ部３０１に外部装置４０が接続されているか否かを検出する。

【０２４５】

ステップＳ２７０２において、画像検証装置２０の制御/演算処理部３０３及び外部装置４０の制御/演算処理部３０６とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。この相互認証は、第５の実施例に示す図２２と同様の手順で実行される。

【０２４６】

ステップＳ２７０３、Ｓ２７０４の処理は、上述の第７の実施例のステップＳ２３０１、Ｓ２３０２と同様の処理としてその説明を省略する。

【０２４７】

ステップＳ２７０５において、制御／演算部３０３は、外部Ｉ／Ｆ部３０１を介して入力された外部装置４０の持つ固有の秘密情報をメモリ３１３に格納し、ディジタル署名データの生成に必要な秘密情報として管理する。

【０２４８】

ステップＳ２７０６において、制御／演算部３０３（に含まれる演算回路３１２）は、上述の秘密情報とＪＰＥＧデータとを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路３１２は、第７の実施例のステップＳ２３０４と同様の演算処理を行う。

【０２４９】

ステップＳ２７０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０６の演算結果をハッシュ関数演算する。ここで、演算回路３１２は、第７の実施例のステップＳ２３０５と同様の演算処理を行う。

【０２５０】

ステップＳ２７０８において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０７の演算結果と、選択されたＪＰＥＧデータとセットで入力されたディジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【０２５１】

ステップＳ２７０９において、表示部３０４は、ステップＳ２７０８の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２５２】

尚、図２７に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２５３】

以上の手順により、選択されたＪＰＥＧデータの正当性を確認した場合、ユーザは、操作部３０６を操作し、該ＪＰＥＧデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路３１０は各処理回路を制御し、該ＪＰＥＧデータを廃棄することもできる。

【０２５４】

以上説明したように、第１１の実施例では、第５の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データの正当性を簡単な構成で、高速に確認することができる。又、上述のディジタル署名データを用いて、ある画像データがどの外部機器或いはどのユーザにて撮像されたかを特定することもできる。

【０２５５】

（第１２の実施例）

第１２の実施例では、画像検証装置２０が、第６の実施例に基づいて生成されたディジタル署名データを用いて、ＪＰＥＧデータの正当性を確認する構成について説明する。

【０２５６】

以下、図２７を用いて第１１の実施例の処理手順の一例について説明する。

【０２５７】

ステップＳ２７０１～Ｓ２７０４の処理は、上述の第１１の実施例と同様の処

理としてその説明を省略する。

【０２５８】

ステップＳ２７０５において、制御／演算部３０３は、画像入力装置１０の持つ固有の秘密情報をメモリ３１３から読み出し、外部装置４０の持つ固有の秘密情報を外部Ｉ／Ｆ部３０１を介して入力する。そして、第６の実施例と同様に、これらの秘密情報を結合させ、新しい秘密情報を生成する。

【０２５９】

ステップＳ２７０６において、制御／演算部３０３（に含まれる演算回路３１２）は、上述の秘密情報とＪＰＥＧデータとを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路３１２は、第７の実施例のステップＳ２３０４と同様の演算処理を行う。

【０２６０】

ステップＳ２７０７において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０６の演算結果をハッシュ関数演算する。ここで、演算回路３１２は、第７の実施例のステップＳ２３０５と同様の演算処理を行う。

【０２６１】

ステップＳ２７０８において、制御／演算部３０３（に含まれる演算回路３１２）は、ステップＳ２７０７の演算結果と、選択されたＪＰＥＧデータとセットで入力されたディジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、ＪＰＥＧデータを正当なものと判断し、一致しなかった場合には、ＪＰＥＧデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【０２６２】

ステップＳ２７０９において、表示部３０４は、ステップＳ２７０８の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したＪＰＥＧデータの正当性を視覚的に分かり易く認識することができる。

【０２６３】

尚、図２７に示す一連の処理手順を制御するプログラムは、ＲＯＭ３０５に格

納されている。このプログラムは、制御／演算部３０３（に含まれる制御回路３１２）によって読み出され、所望の画像の検証を指示する毎に起動する。

【０２６４】

以上の手順により、選択されたＪＰＥＧデータの正当性を確認した場合、ユーザは、操作部３０６を操作し、該ＪＰＥＧデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路３１０は各処理回路を制御し、該ＪＰＥＧデータを廃棄することもできる。

【０２６５】

以上説明したように、第１２の実施例では、第６の実施例の画像入力装置１０にて撮像され、高能率符号化されたディジタル画像データの正当性を簡単な構成で、高速に確認することができる。又、上述のディジタル署名データを用いて、ある画像データがどの外部機器と接続された画像入力装置或いはどのユーザによって使用された画像入力装置にて撮像されたかを特定することもできる。

【０２６６】

尚、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【０２６７】

例えば、第１～第６の実施例では、画像入力装置１０内においてディジタル署名データを生成したが、該ディジタル署名データを画像入力装置１０に接続された外部装置４０にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、高能率符号化されたディジタル画像データ等を画像入力装置１０から外部装置４０に送信し、生成処理を開始する。

【０２６８】

又、第１～第６の実施例では、ディジタル署名データの生成に必要な演算処理を画像入力装置１０と外部装置４０とに分散させ、各装置が共同してディジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、高能率符号化されたディジタル画像データ等の中で必要な部分のみを画像入力装

置１０から外部装置４０に送信し、生成処理を開始する。

【０２６９】

又、第７～第１２の実施例では、画像検証装置２０が外部入力されたディジタル画像データを用いてディジタル署名データを生成したが、該ディジタル署名データを画像検証装置２０に接続された外部装置４０にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、外部入力されたディジタル画像データ等を画像検証装置２０から外部装置４０に送信し、生成処理を開始する。

【０２７０】

又、第７～第１２の実施例では、ディジタル署名データの生成に必要な演算処理を画像検証装置２０と外部装置４０とに分散させ、各装置が共同してディジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、ディジタル署名データの生成に必要な処理プログラム、外部入力されたディジタル画像データ等の中で必要な部分のみを画像検証装置２０から外部装置４０に送信し、生成処理を開始する。

【０２７１】

又、第７～第１２の実施例では、図２４～図２７に示す一連の処理手順を制御するプログラムは、所望の画像の検証を指示する毎に起動する構成として説明したが、所望の画像を外部入力することに自動的に起動するように構成してもよい。

【０２７２】

従って、前述の実施例はあらゆる点おいて単なる例示に過ぎず、限定的に解釈してはならない。

【０２７３】

【発明の効果】

以上のように、本発明によれば、ディジタルデータの著作権を保護すると共に、そのディジタルデータに対する不正な処理（改竄、偽造、合成等）を検出するための署名データを簡単な構成で、高速に生成することができる。又、その署名データを用いて、ディジタルデータに対する不正な処理（改竄、偽造、合成等）

を簡単な構成で、高速且つ確実に検出することができる。

【０２７４】

又、本発明によれば、ディジタルデータとそのディジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるディジタルデータがどの機器によって生成されたかを特定することができる。

【０２７５】

又、本発明によれば、ディジタルデータとそのディジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるディジタルデータがどの機器によって生成されたかを特定することができる。

【０２７６】

又、本発明によれば、ディジタルデータとそのディジタルデータを生成した機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるディジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

【０２７７】

又、本発明によれば、ディジタルデータとそのディジタルデータを生成した機器の秘密情報とその機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるディジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

【図面の簡単な説明】

【図１】

本実施例のディジタル画像検証システムについて説明する図。

【図２】

本実施例の画像入力装置１０の基本構成について説明するブロック図。

【図３】

本実施例の画像検証装置２０の基本構成について説明するブロック図。

【図４】

第１の実施例の処理手順を説明するフローチャート。

【図５】

第１の実施例における所定の演算処理を説明する図。

【図６】

第２の実施例の処理手順を説明するフローチャート。

【図７】

第２の実施例におけるＪＰＥＧデータを表す図。

【図８】

第２の実施例における秘密情報を説明する図。

【図９】

第２の実施例における所定の演算処理を説明する図。

【図１０】

第２の実施例におけるハッシュ関数演算の第１のモードを説明する図。

【図１１】

第２の実施例におけるハッシュ関数演算の第２のモードを説明する図。

【図１２】

第２の実施例におけるハッシュ関数演算の第３のモードを説明する図。

【図１３】

第１～第３のモードにおける使用される初期値を説明する図。

【図１４】

第３の実施例の処理手順を説明するフローチャート。

【図１５】

第３の実施例における秘密情報を説明する図。

【図１６】

第３の実施例におけるＣＢＣモードを説明する図。

【図１７】

第３の実施例におけるＣＦＢモードを説明する図。

【図１８】

第３の実施例におけるＯＦＢモードを説明する図。

【図１９】

第４の実施例の処理手順を説明するフローチャート。

【図２０】

第４の実施例における秘密情報を説明する図。

【図２１】

第５、第６の実施例の処理手順を説明するフローチャート。

【図２２】

画像入力装置１０と外部装置４０との相互認証処理を説明する図。

【図２３】

第７の実施例の処理手順を説明するフローチャート。

【図２４】

第８の実施例の処理手順を説明するフローチャート。

【図２５】

第９の実施例の処理手順を説明するフローチャート。

【図２６】

第１０の実施例の処理手順を説明するフローチャート。

【図２７】

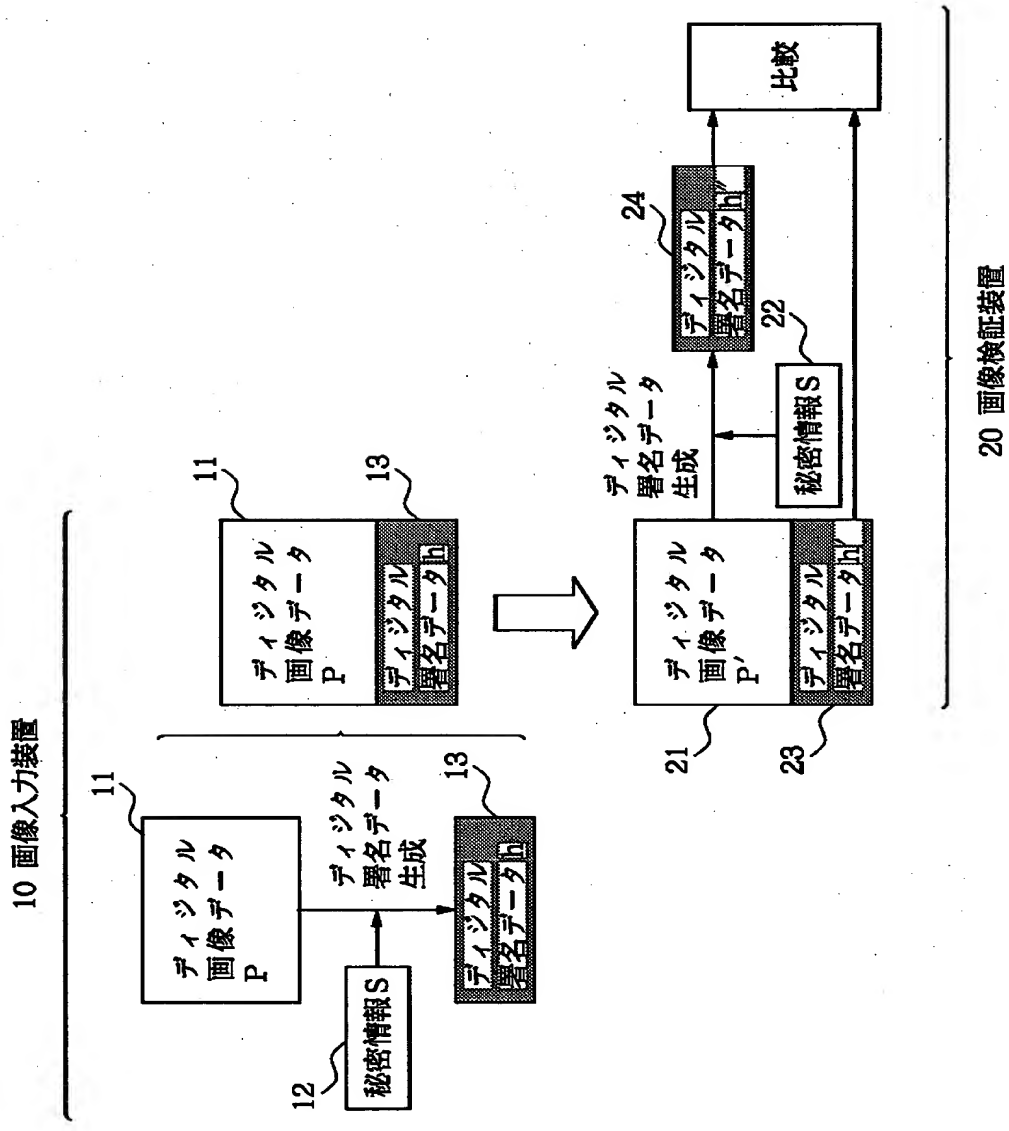
第１２の実施例の処理手順を説明するフローチャート。

【図２８】

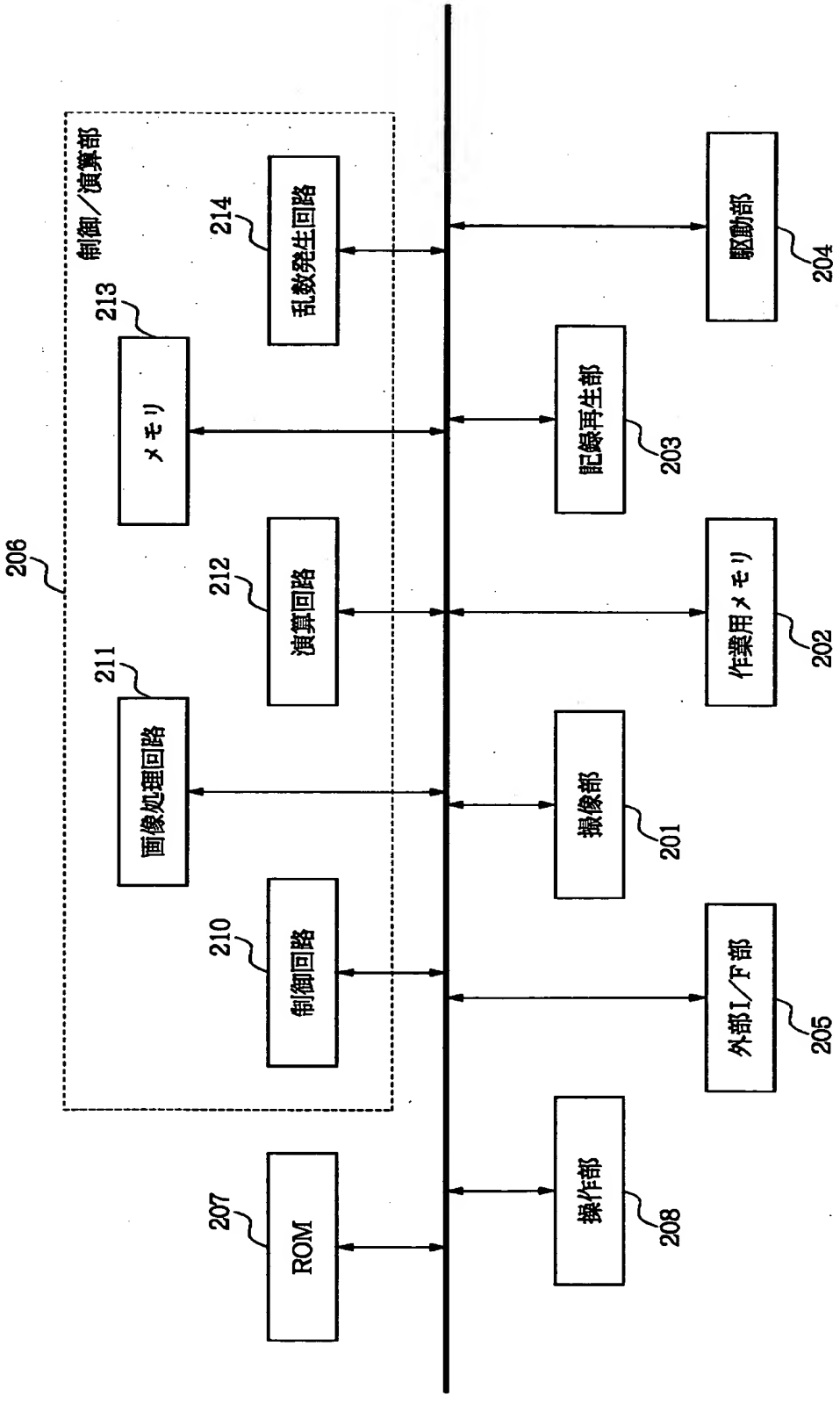
従来のシステムを説明する図。

【書類名】　　図面

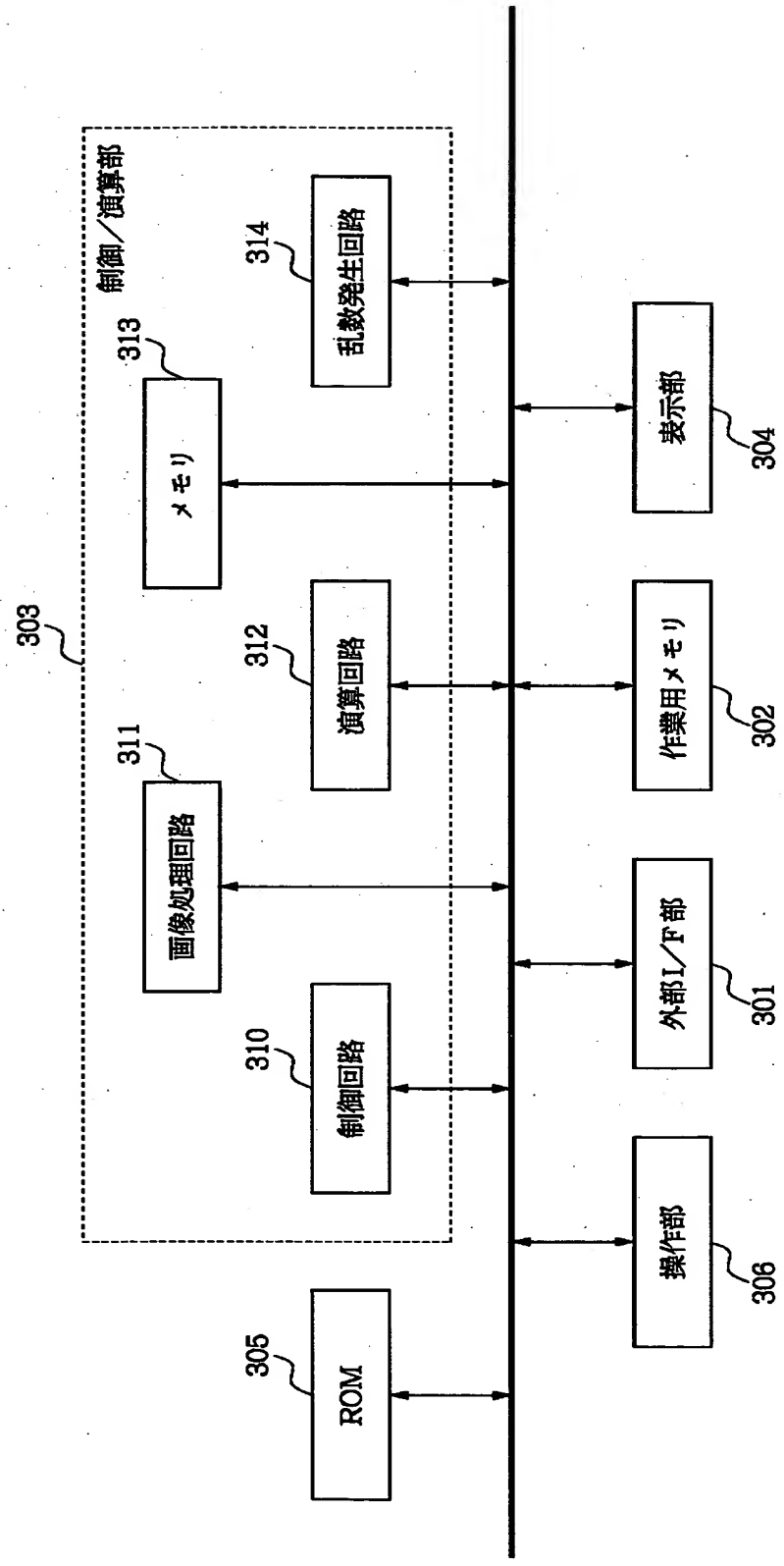
【図１】


10 画像入力装置
11
ディジタル
画像データ
P
ディジタル
署名データ生成
12
秘密情報S
13
ディジタル
署名データh
11
ディジタル
画像データ
P
13
ディジタル
署名データh
ディジタル
署名データ生成
秘密情報S
22
24
ディジタル
署名データh'
比較
ディジタル
画像データ
P'
21
ディジタル
署名データh'
23
20 画像検証装置

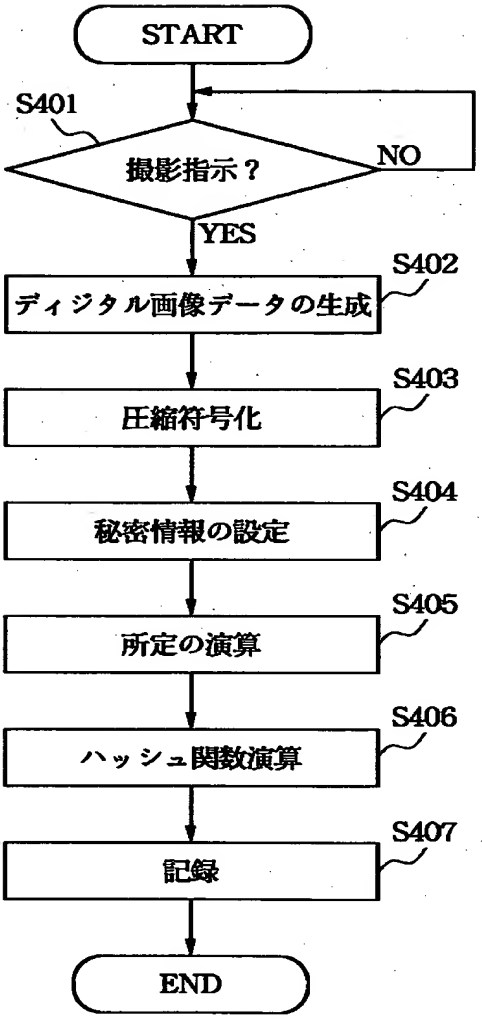
【図２】


制御／演算部
206
213
メモリ
214
乱数発生回路
212
演算回路
211
画像処理回路
210
制御回路
207
ROM
駆動部
204
記録再生部
203
作業用メモリ
202
撮像部
201
外部I／F部
205
操作部
208

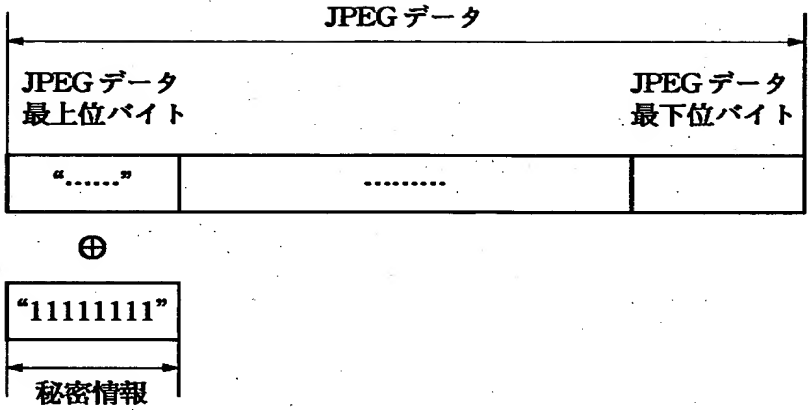
【図３】


制御／演算部
303
313
メモリ
314
乱数発生回路
312
演算回路
311
画像処理回路
310
制御回路
305
ROM
表示部
304
作業用メモリ
302
外部I／F部
301
操作部
306

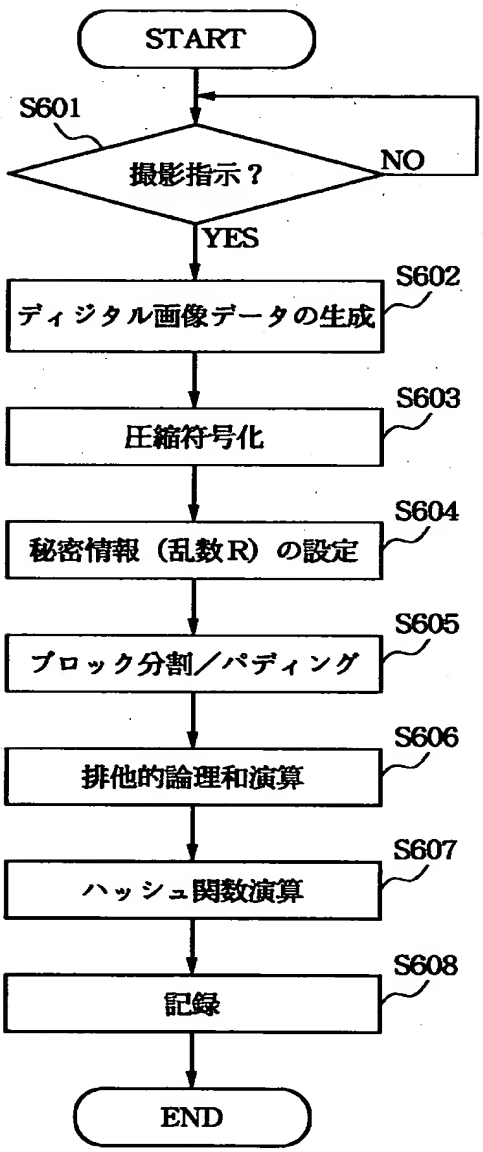
【図４】


START
S401
撮影指示？
NO
YES
S402
ディジタル画像データの生成
S403
圧縮符号化
S404
秘密情報の設定
S405
所定の演算
S406
ハッシュ関数演算
S407
記録
END

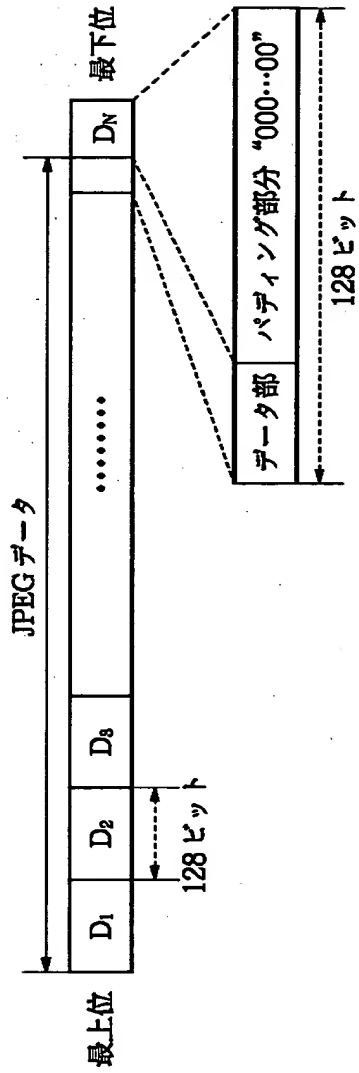
【図５】



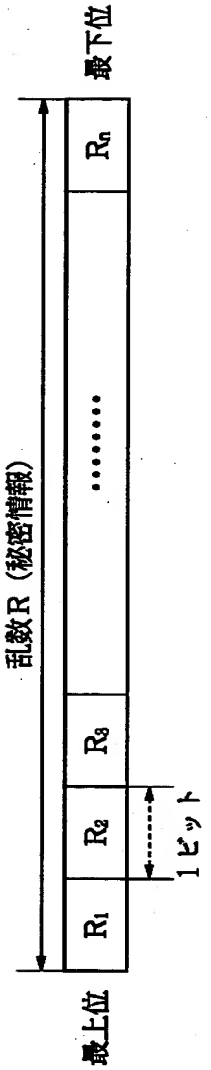
【図６】


START
S601
撮影指示？
NO
YES
S602
ディジタル画像データの生成
S603
圧縮符号化
S604
秘密情報（乱数R）の設定
S605
ブロック分割／パディング
S606
排他的論理和演算
S607
ハッシュ関数演算
S608
記録
END

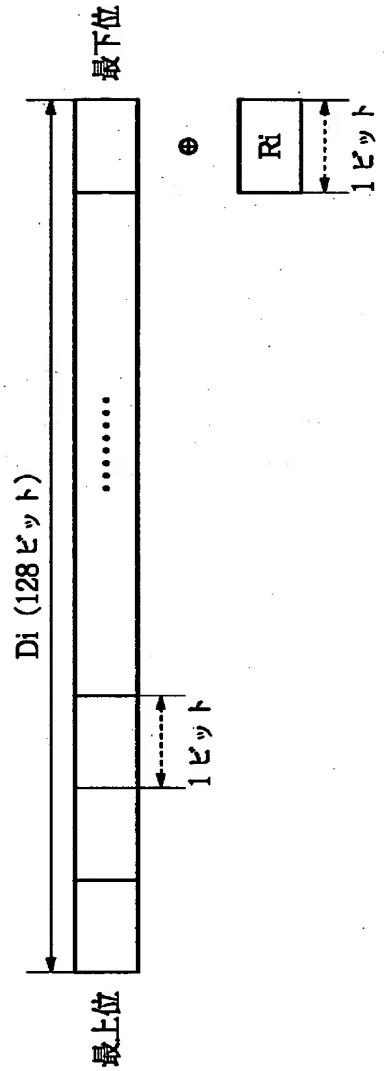
【図７】



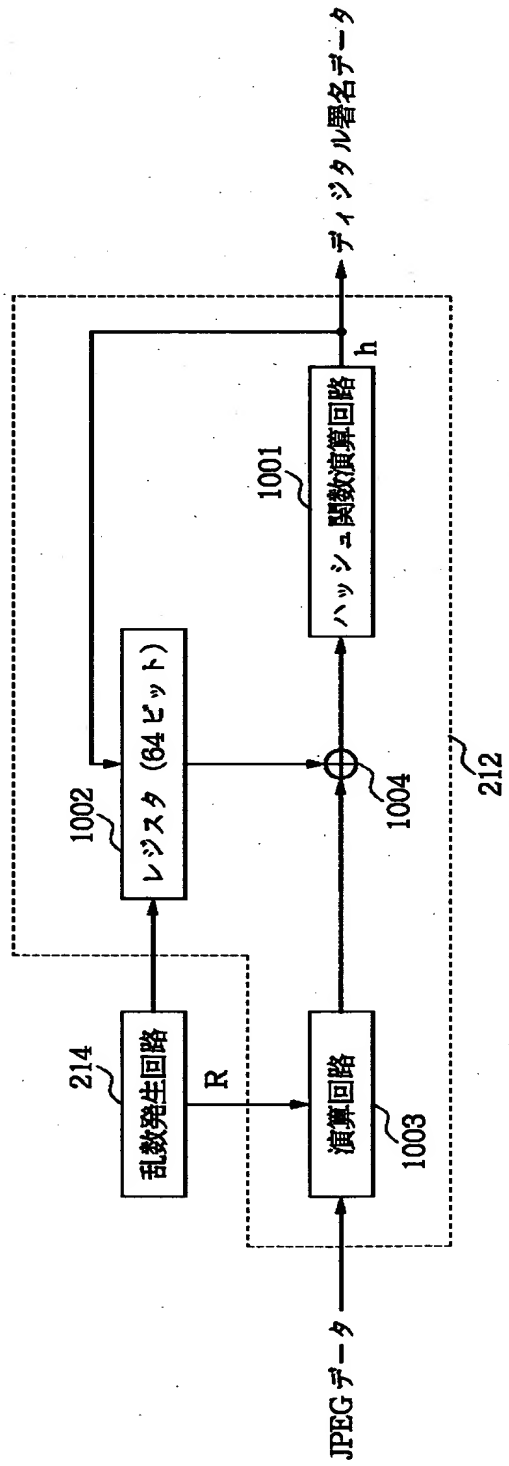
【図８】



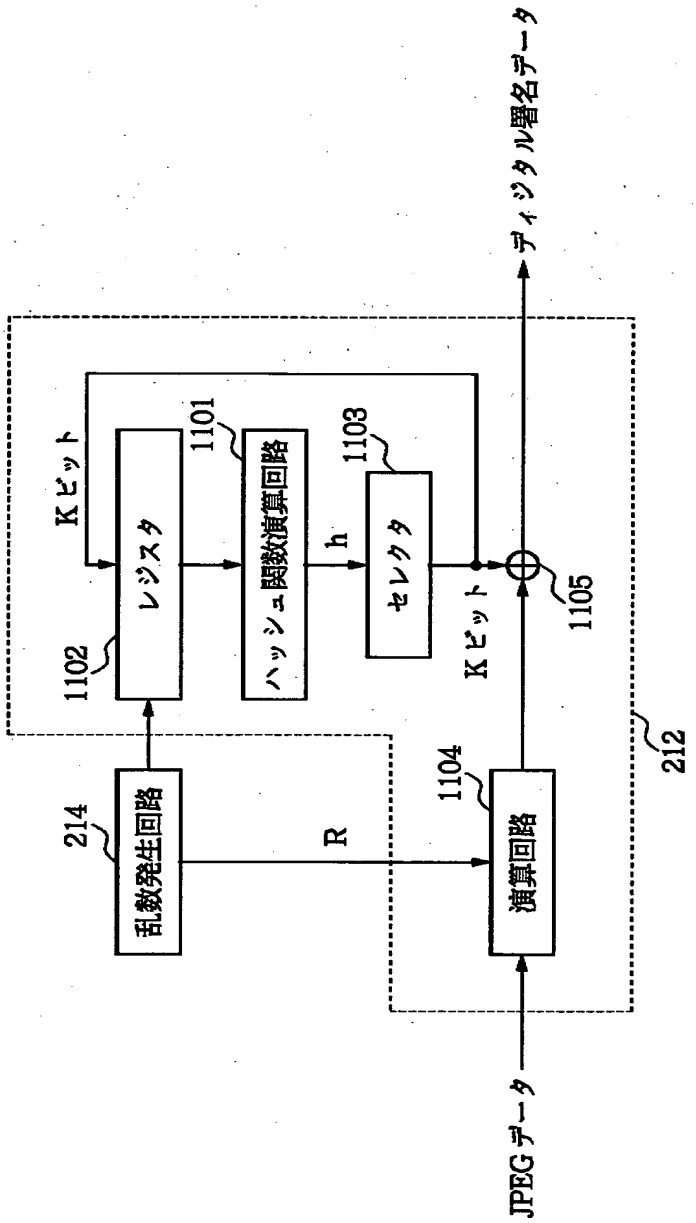
【図９】



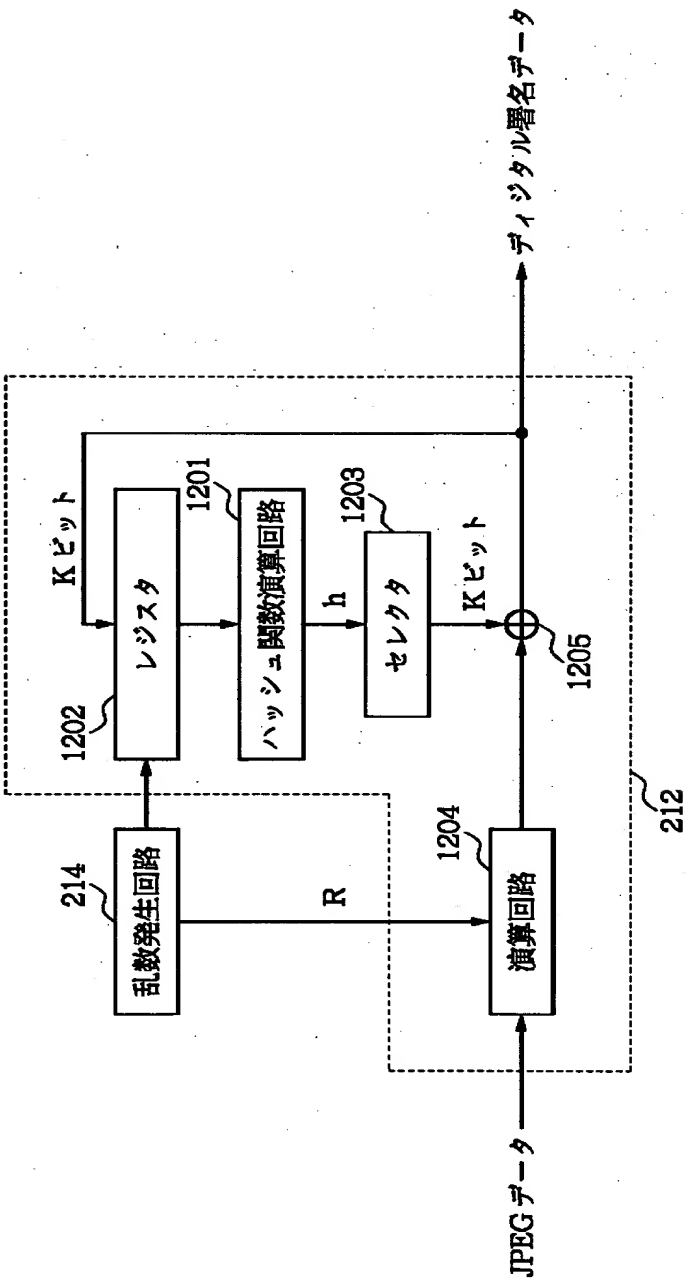
【図１０】


ディジタル署名データ
h
ハッシュ関数演算回路
1001
レジスタ（64ビット）
1002
1004
212
乱数発生回路
214
R
演算回路
1003
JPEGデータ

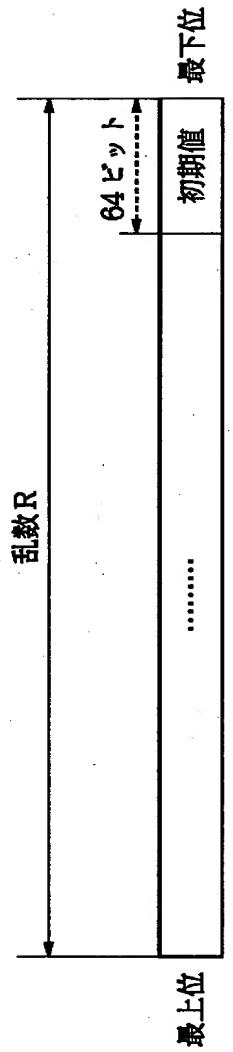
【図１１】


ディジタル署名データ
Kビット
1101
1103
レジスタ
ハッシュ関数演算回路
h
セレクタ
1102
Kビット
1105
212
1104
214
乱数発生回路
R
演算回路
JPEGデータ

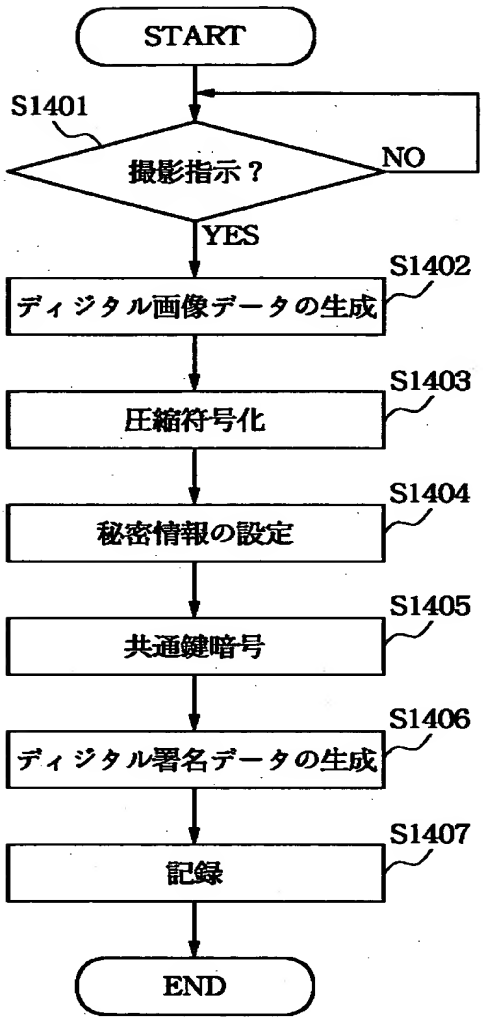
【図１２】


ディジタル署名データ
Kビット
1201
1203
レジスタ
ハッシュ関数演算回路
h
セレクタ
Kビット
1205
1202
212
1204
214
乱数発生回路
R
演算回路
JPEGデータ

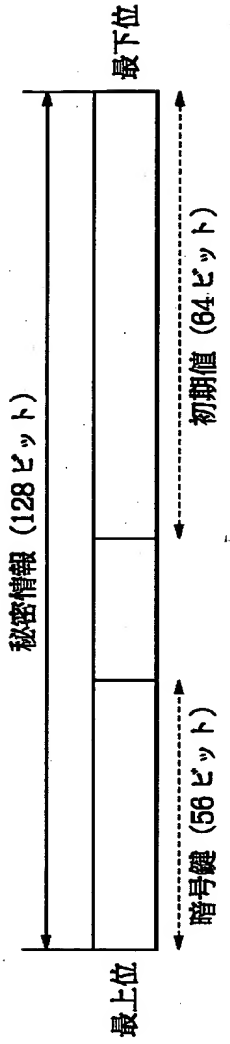
【図１３】



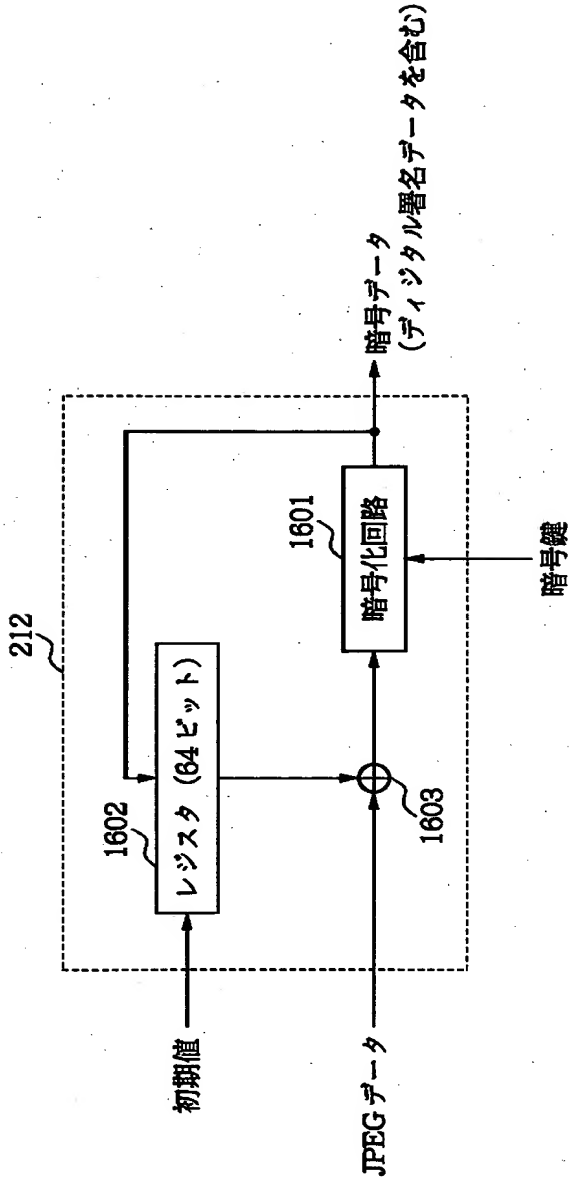
【図１４】


START
S1401
撮影指示？
NO
YES
S1402
ディジタル画像データの生成
S1403
圧縮符号化
S1404
秘密情報の設定
S1405
共通鍵暗号
S1406
ディジタル署名データの生成
S1407
記録
END

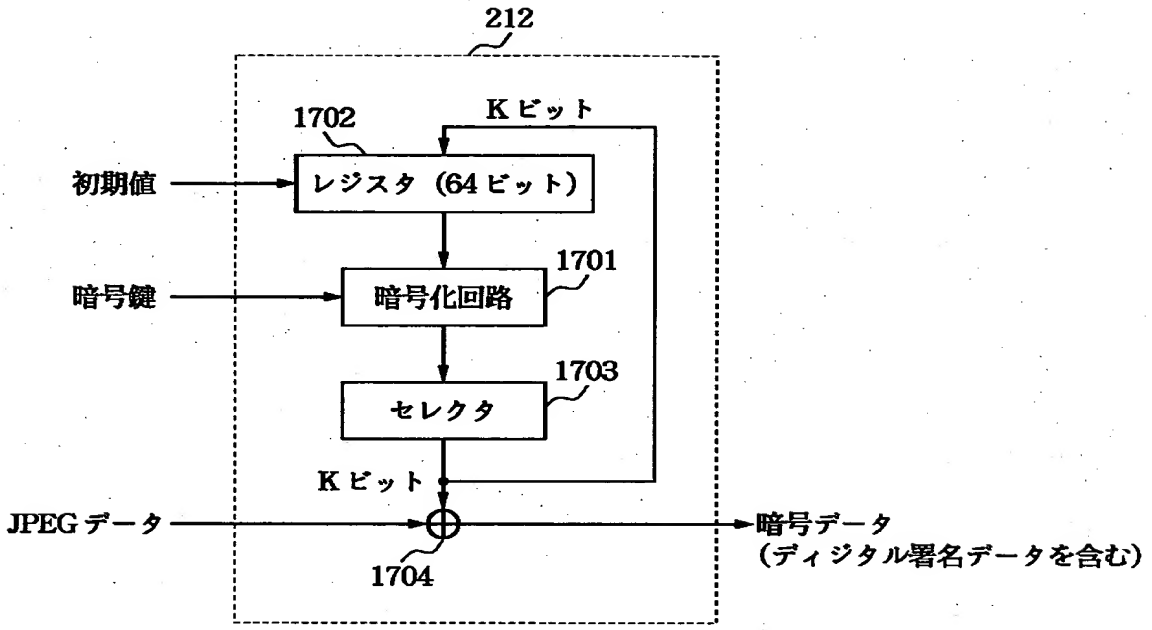
【図１５】



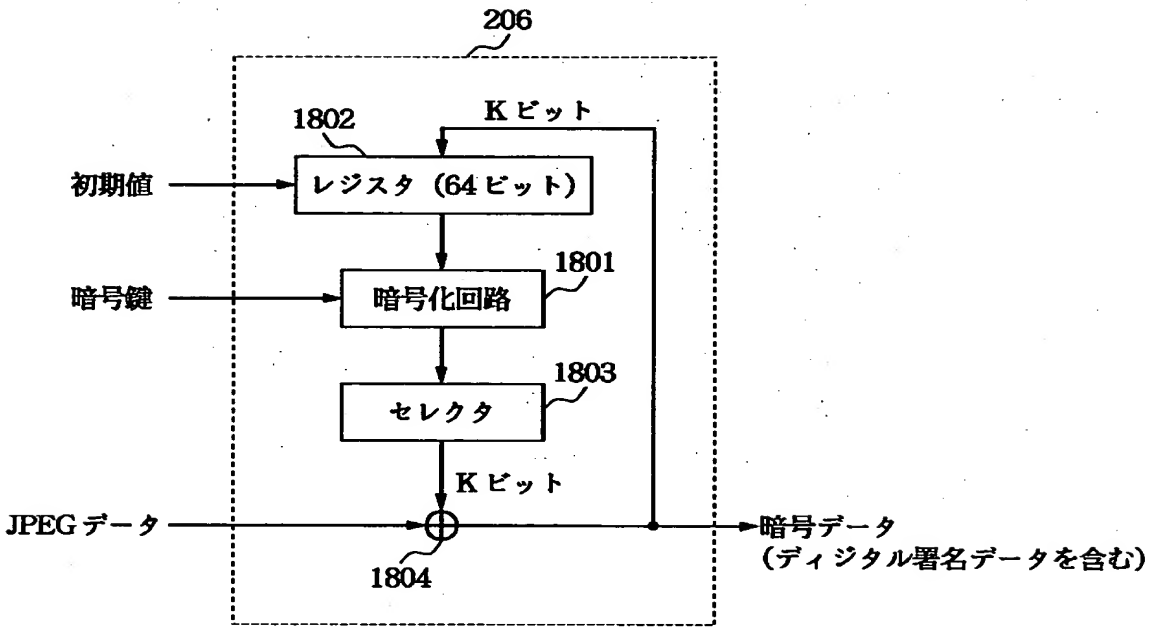
【図１６】


暗号データ
(ディジタル署名データを含む)
212
1601
暗号化回路
暗号鍵
1602
レジスタ (64ビット)
1603
初期値
JPEGデータ

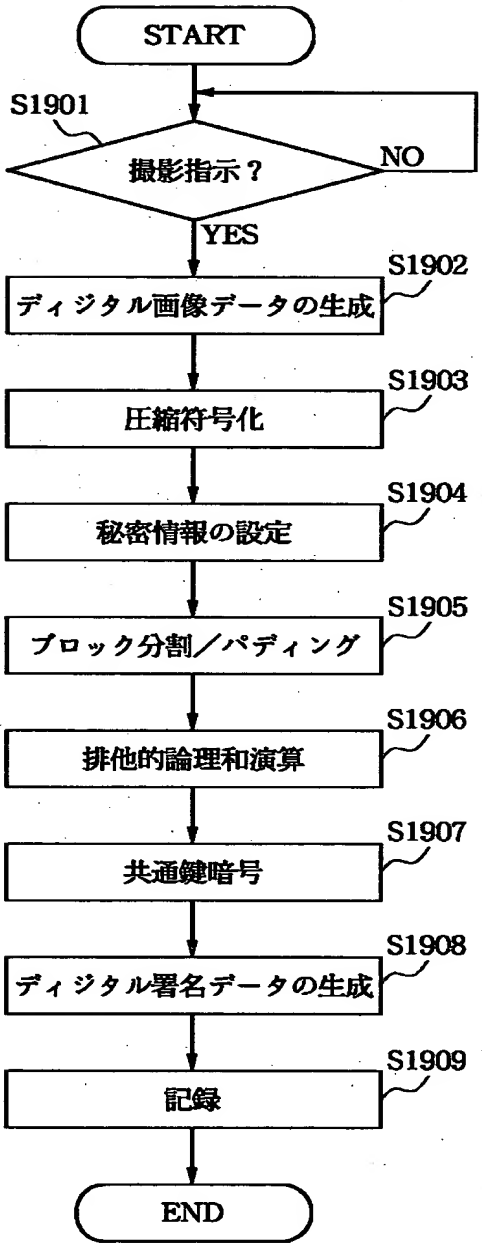
【図１７】


212
1702
Kビット
初期値
レジスタ（64ビット）
暗号鍵
暗号化回路
1701
セレクタ
1703
Kビット
JPEGデータ
暗号データ
（ディジタル署名データを含む）
1704

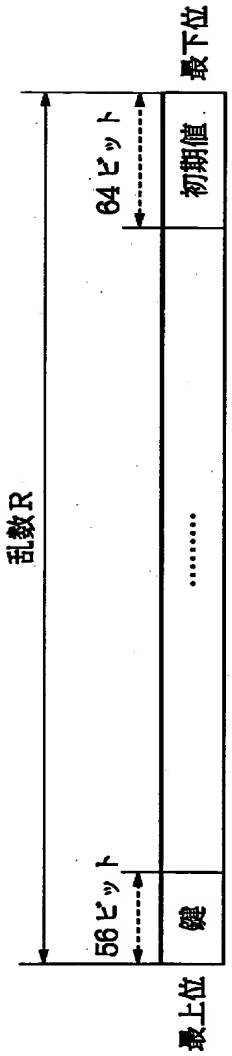
【図１８】


206
1802
Kビット
初期値
レジスタ（64ビット）
1801
暗号鍵
暗号化回路
1803
セレクタ
Kビット
JPEGデータ
暗号データ
（ディジタル署名データを含む）
1804

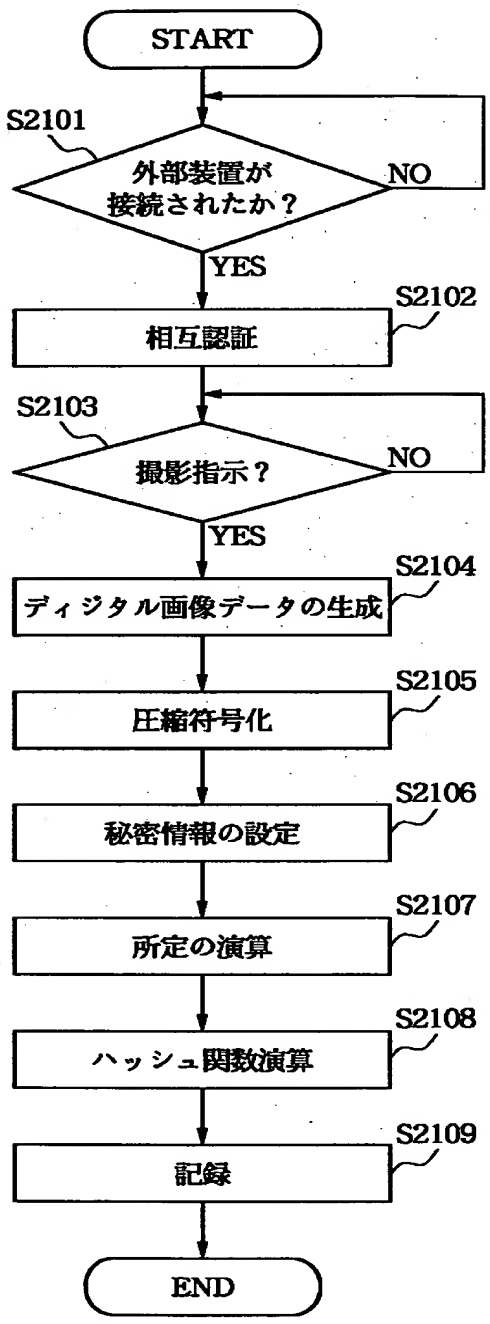
【図１９】


START
S1901
撮影指示？
NO
YES
S1902
ディジタル画像データの生成
S1903
圧縮符号化
S1904
秘密情報の設定
S1905
ブロック分割／パディング
S1906
排他的論理和演算
S1907
共通鍵暗号
S1908
ディジタル署名データの生成
S1909
記録
END

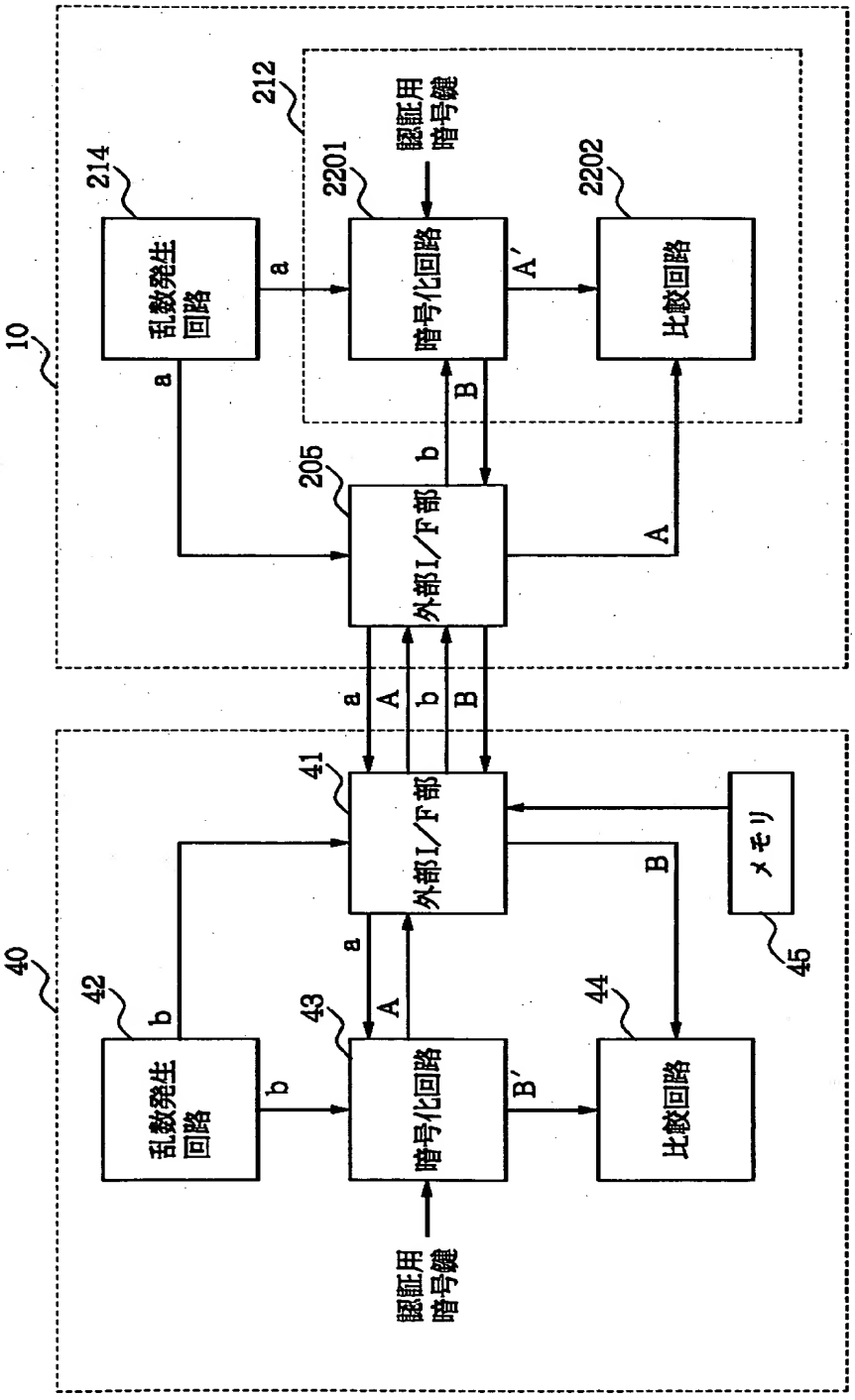
【図２０】



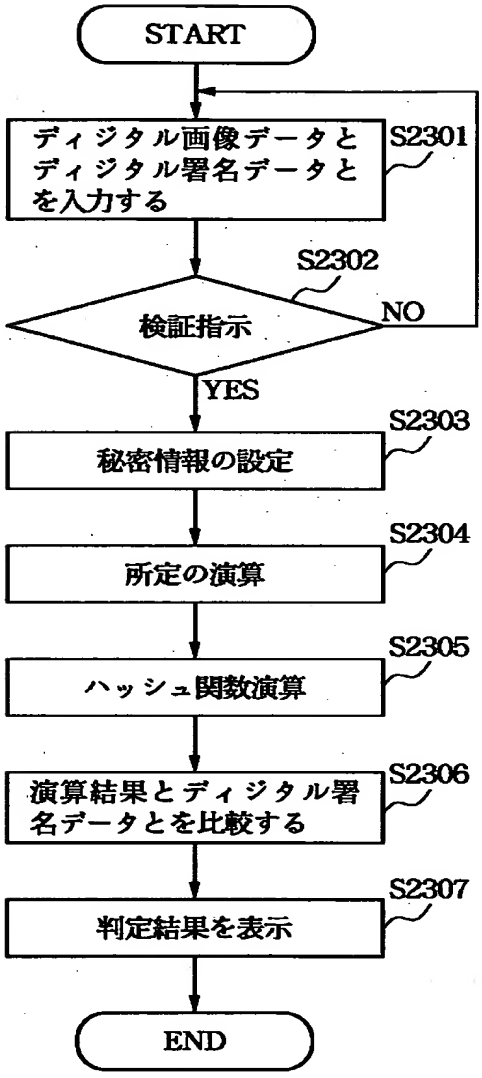
【図２１】


START
S2101
外部装置が
接続されたか？
NO
YES
S2102
相互認証
S2103
撮影指示？
NO
YES
S2104
ディジタル画像データの生成
S2105
圧縮符号化
S2106
秘密情報の設定
S2107
所定の演算
S2108
ハッシュ関数演算
S2109
記録
END

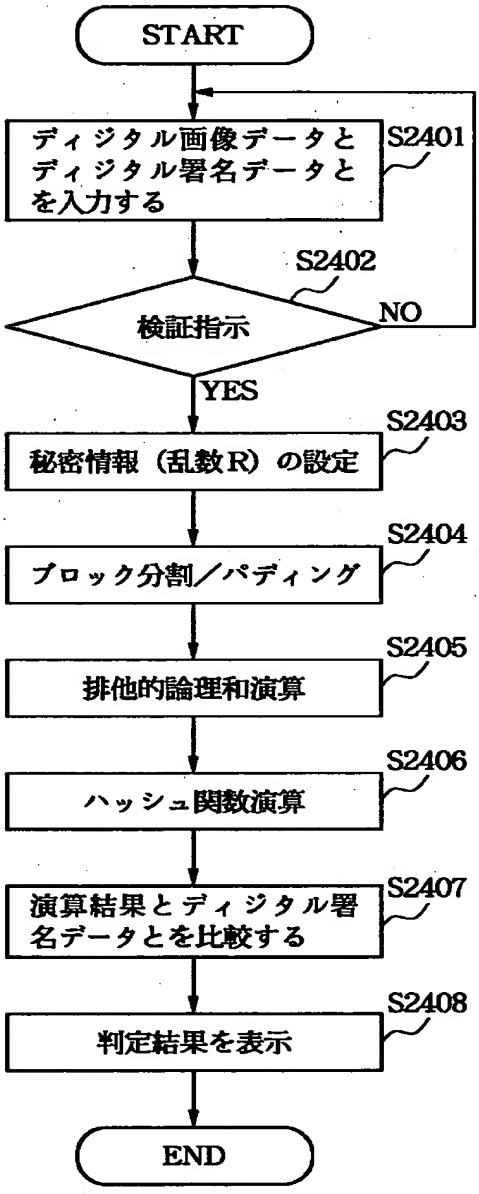
【図２２】


10
212
214
2201
2202
205
41
40
42
43
44
45
乱数発生回路
暗号化回路
比較回路
外部I/F部
メモリ
認証用暗号鍵
a
b
A
B
A′
B′

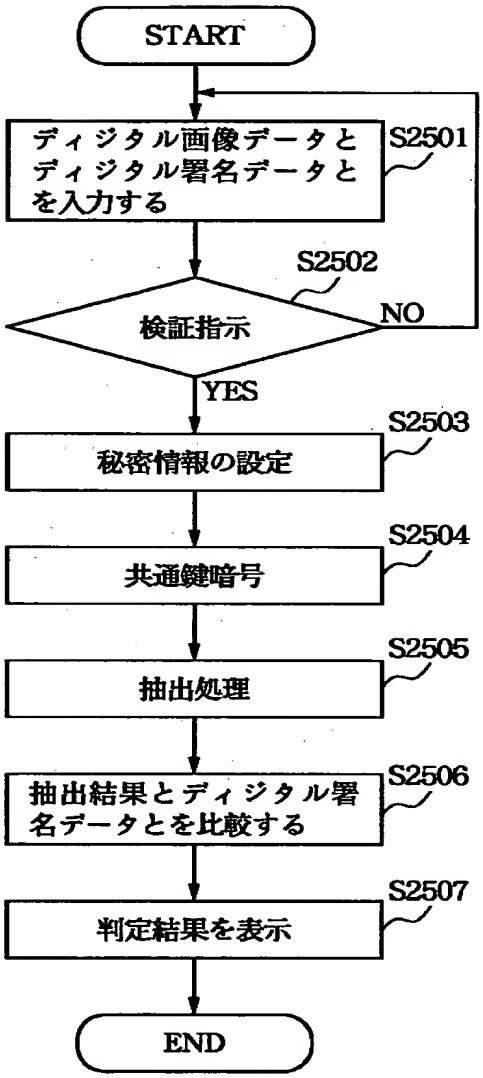
【図２３】


START
ディジタル画像データとディジタル署名データとを入力する
S2301
S2302
検証指示
NO
YES
S2303
秘密情報の設定
S2304
所定の演算
S2305
ハッシュ関数演算
S2306
演算結果とディジタル署名データとを比較する
S2307
判定結果を表示
END

【図２４】

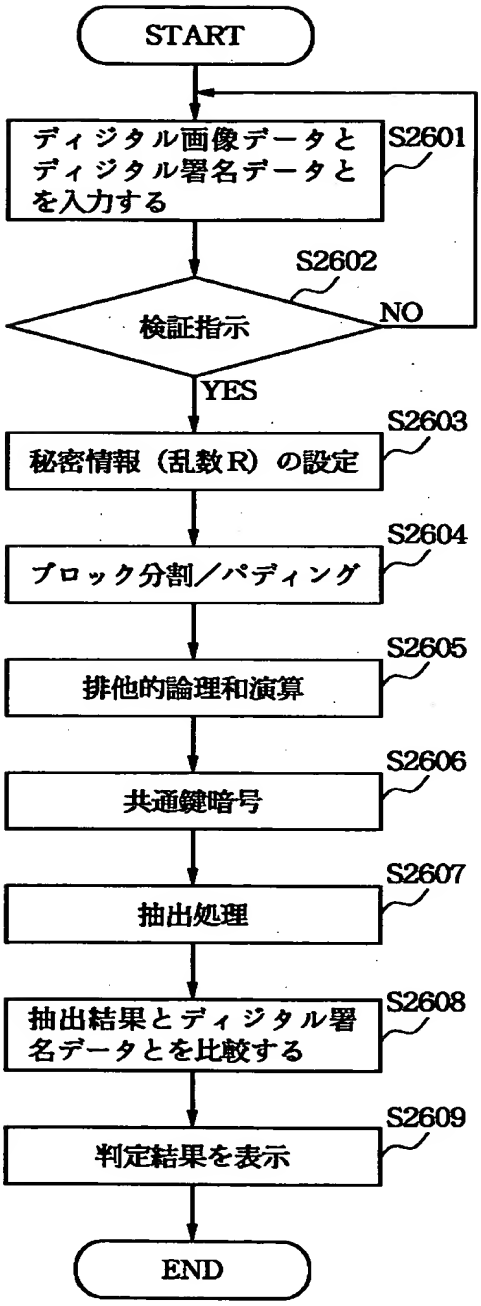

START
ディジタル画像データとディジタル署名データとを入力する
S2401
S2402
検証指示
NO
YES
S2403
秘密情報（乱数R）の設定
S2404
ブロック分割／パディング
S2405
排他的論理和演算
S2406
ハッシュ関数演算
S2407
演算結果とディジタル署名データとを比較する
S2408
判定結果を表示
END

【図２５】

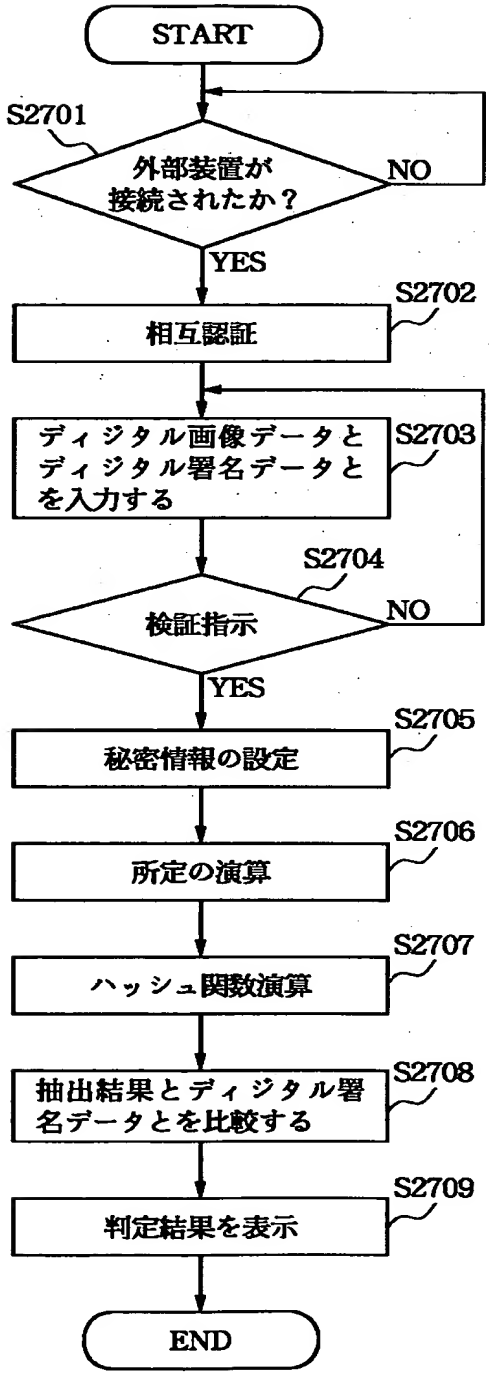


出証特２０００－３０２２３８２

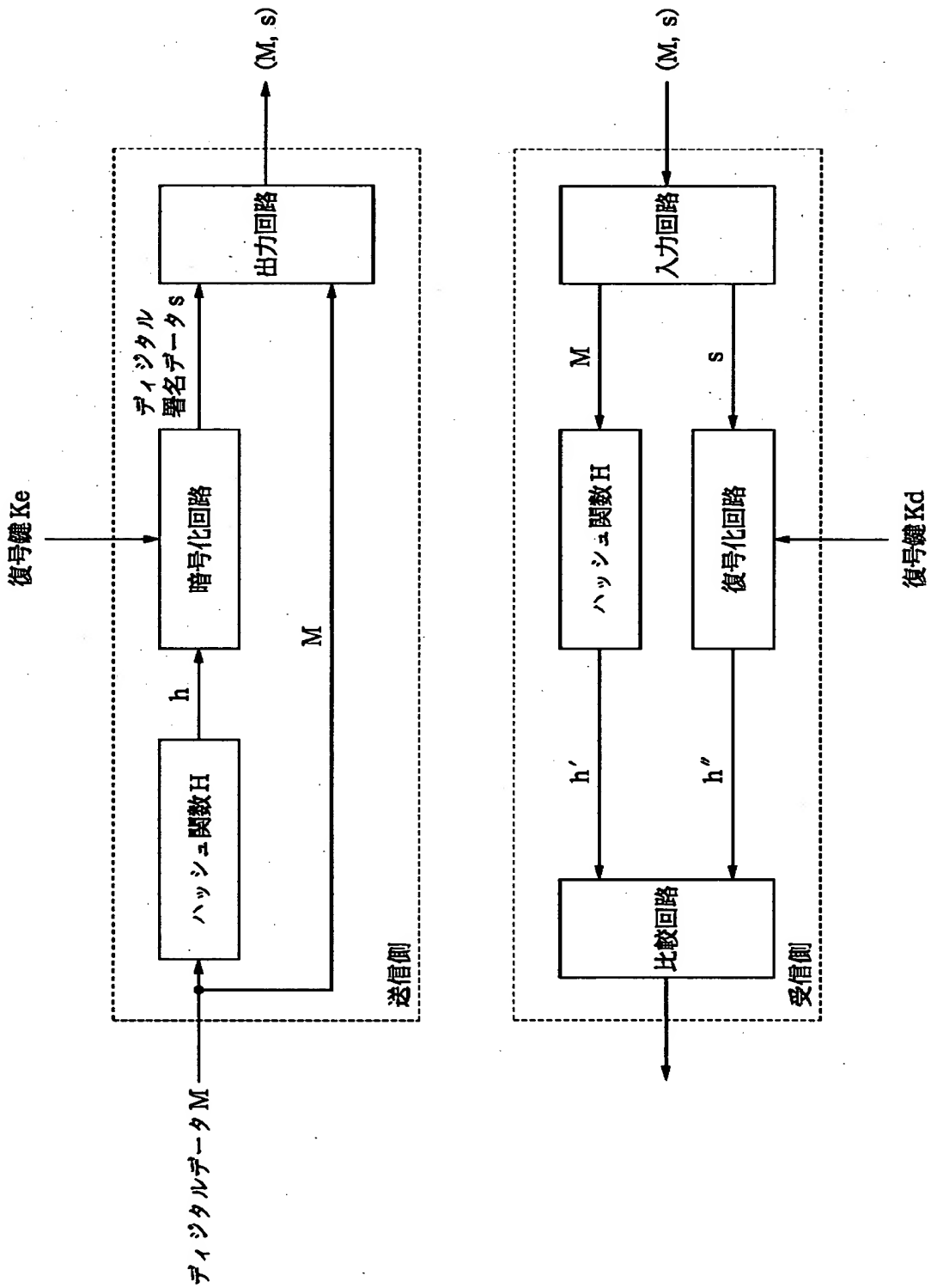
【図２６】


START
ディジタル画像データとディジタル署名データとを入力する
S2601
S2602
検証指示
NO
YES
秘密情報（乱数R）の設定
S2603
ブロック分割／パディング
S2604
排他的論理和演算
S2605
共通鍵暗号
S2606
抽出処理
S2607
抽出結果とディジタル署名データとを比較する
S2608
判定結果を表示
S2609
END

【図２７】


START
S2701
外部装置が
接続されたか？
NO
YES
S2702
相互認証
ディジタル画像データと
ディジタル署名データと
を入力する
S2703
S2704
検証指示
NO
YES
S2705
秘密情報の設定
S2706
所定の演算
S2707
ハッシュ関数演算
抽出結果とディジタル署
名データとを比較する
S2708
S2709
判定結果を表示
END

【図２８】


(M, s)
出力回路
ディジタル
署名データs
暗号化回路
復号鍵Ke
ハッシュ関数H
h
M
送信側
ディジタルデータM
(M, s)
入力回路
M
s
ハッシュ関数H
復号化回路
復号鍵Kd
h′
h″
比較回路
受信側

【書類名】　　要約書

【要約】

【課題】　ディジタルデータの正当性を検証することのできる技術を提供する。

【解決手段】　第１の画像処理装置１０は、ディジタル画像１１と秘密情報１２とを用いて所定の演算を行い、その演算結果を用いて該ディジタル画像に対する不正な処理を検出するため署名データ１３を生成する。第２の画像処理装置２０は、そのディジタル画像１１と秘密情報２２とを用いて所定の演算を行い、その演算結果と上述の署名データ１３とを比較してそのディジタル画像１１に対する不正な処理の有無を検出する。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００１００７〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社